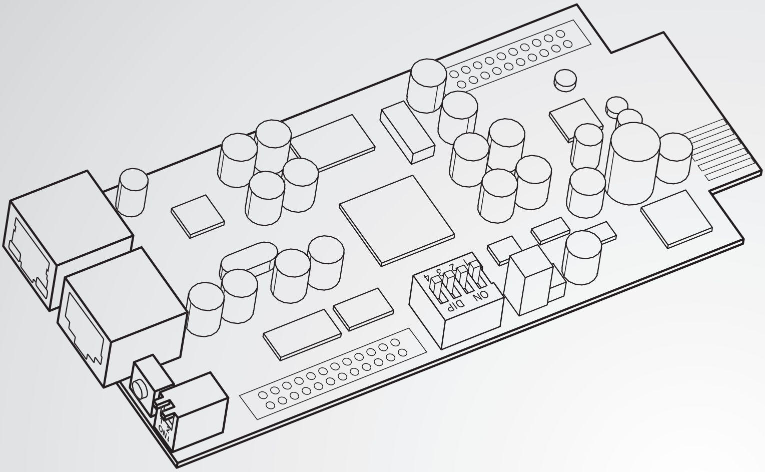


The power behind competitiveness

Delta InsightPower SNMP IPv6 for PDC

User Manual

www.deltapowersolutions.com

Save This Manual

This manual contains important instructions and warnings that you should follow during the installation, operation, storage and maintenance of this product. Failure to heed these instructions and warnings will void the warranty.

Given that Delta will continuously improve and develop the product, changes may be made to the information in this Manual at any time without obligation to notify any person of such revision or changes. Delta will make all possible efforts to secure the accuracy and the integrity of this Manual. Delta disclaims any kinds or forms of warranty, guarantee, or undertaking, either expressly or implicitly, including but not limited to the completeness, faultlessness, accuracy, non-infringement, merchantability or fitness for a particular purpose of the Manual.

Table of Contents

Chapter 1 : Important Safety Instructions

1-1 Warnings

- The InsightPower SNMP IPv6 for PDC, hereafter referred to as SNMP IPv6, is designed to work with a PDC (Power Distribution Cabinet). It needs to be installed in the PDC's SNMP slot.
- Do not place or use this unit in the presence of flammable substances.
- Do not attempt to disassemble the unit.
- Do not attempt to perform any internal modifications on the unit.
- Do not attempt to fix/ replace internal components. When repair is needed, refer all servicing to your local dealer or service personnel.
- Do not allow any objects or liquids of any kind to penetrate the unit.
- Always follow this User Manual to install and operate this unit.
- Do not play the included CD with a conventional CD player. This could generate loud noise at a level that could result in permanent hearing loss.

1-2 Standard Compliance

- **EN 55022: 2006 + A1: 2007, Class A**

  EN 61000-3-3: 1995+A1: 2001+A2: 2005

- **EN 55024: 1998 + A1: 2001 + A2: 2003**

  IEC 61000-4-2: 1995+A1: 1998+A2: 2000

  IEC 61000-4-3: 2006

  IEC 61000-4-4: 2004

  IEC 61000-4-5: 2005

  IEC 61000-4-6: 2007

  IEC 61000-4-8: 1993+A1: 2000

  IEC 61000-4-11: 2004

Chapter 2 : Introduction

2-1 Product Description

The InsightPower SNMP IPv6 for PDC is an intelligent device that serves as an interface between the PDC and your network. It communicates with the PDC to obtain readings, settings and status information from system, panel and branch circuits. With its user-friendly web interface that features instant monitoring and management, you can easily manage your PDC and SNMP IPv6. It supports a wide range of common protocols, including SNMPv3, HTTP, SFTP and Telnet.

2-2 Features

- **Remote management and monitoring**

  Manage your PDC from workstations connected in the network.

- **Comprehensive protocol support**

  Including HTTP, HTTPS, SNMPv3, FTP, SFTP and Telnet.

- **Compatible with EnviroProbe**

  Works great with the Delta EnviroProbe (sold separately) to detect environment temperature and dry contact status.

- **Supports encrypted connections**

  Including HTTPS, SSH, SFTP and SNMPv3 to improve connection security.

- **Comprehensive event and data log**

  Show and keep track of PDC' system status, circuit readings and events.

- **Supports IPv6 protocol**

  IPv6 Ready Logo Phase 2 (Core for Host, Logo ID 02-C-000624)

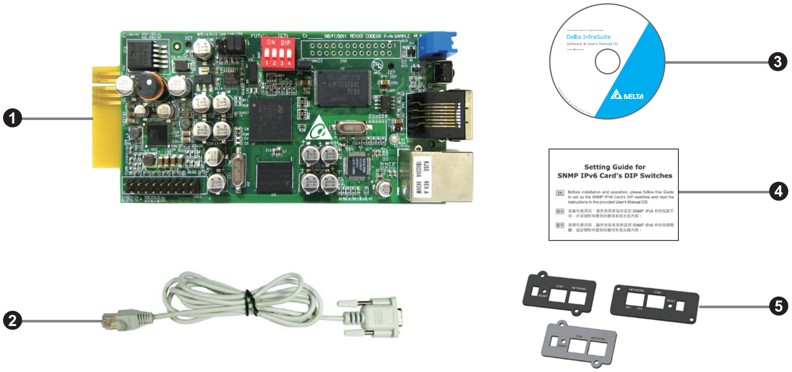
Other features and supported protocols include:

- User notification via SNMP Traps and e-mail
- Network Time Protocol

- BOOTP/ DHCP
- RADIUS (Remote Authentication Dial In User Service) login and local authentication
- Syslog remote event log management

2-3 Package Contents

Please carefully check the SNMP IPv6 and the included accessories. Contact your local dealer if any item is missing or damaged. Should you return any item for any reason, ensure that they are carefully repacked using the original packing materials came with the unit.

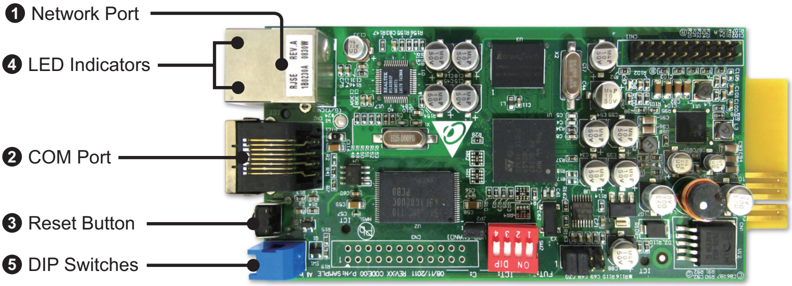


No.	Item	Quantity
❶	InsightPower SNMP IPv6 for PDC	1 PC
❷	RJ45 to DB9 cable	1 PC
❸	Software & User's Manual CD	1 PC
❹	Setting Guide for SNMP IPv6 Card's DIP Switches	1 PC
❺	Cover	3 PCS

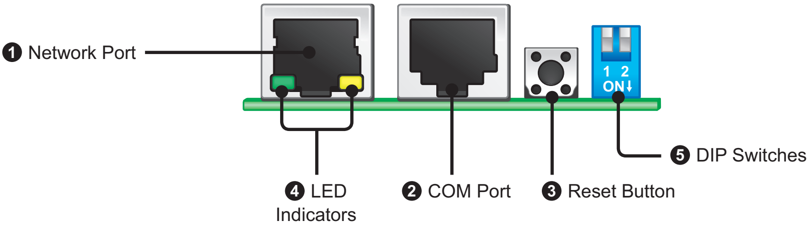
2-4 Interface

On the SNMP IPv6 you can find a Network port, a COM port, LED indicators, a Reset button and DIP switches. Please refer to the table below.

Top view:



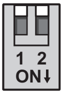
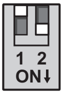
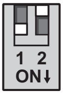
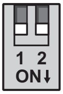
Front view:



No.	Item	Description
❶	Network Port	Connects to the network.
❷	COM Port	1. Connects to a workstation with the provided RJ45 to DB9 cable. 2. Connects to an EnviroProbe (optional).

No.	Item	Description
❸	Reset Button	Resets the SNMP IPv6. This does not affect the PDC.
❹	LED Indicators	When the SNMP IPv6 is initializing or upgrading firmware, the two LED indicators flash simultaneously to show its status. Refer to the following: ● **Rapid simultaneous flashing** (every 50ms) : Initialization or firmware upgrade in progress. ● **Slow simultaneous flashing** (every 500ms) : Initialization failed. **WARNING :** Do **NOT** remove the SNMP IPv6 or disconnect PDC's input power during initialization or firmware upgrade! This could result in data loss or damage to the SNMP IPv6. The green LED indicator shows the network connection status: ● **ON** : Network connection established and the IPv4 address is useable. ● **OFF** : Not connected to a network. ● **Flashes slowly** (every 500ms) : Faulty IP address. The yellow LED indicator shows the linking status between the SNMP IPv6 and the PDC: ● **Flashes rapidly** (every 50ms): PDC linked. ● **Flashes slowly** (every 500ms): PDC not linked.

No.	Item	Description
❺	DIP Switches	Determine the operation modes.

DIP switches	Operation mode	Description
	Normal Mode	The SNMP IPv6 links with the PDC.
	Pass Through Mode	The SNMP IPv6 does not monitor the PDC, but uses its COM port to connect the PDC and the workstation via Modbus protocol (Baud rate: 9600).
	Sensor Mode (with EnviroProbe)	The SNMP IPv6 links with the PDC and EnviroProbe.
	Configuration Mode	Configure your SNMP IPv6 via the COM port. Refer to ***4-4 Configure via COM Port***.

NOTE

To know more about the EnviroProbe, refer to its user manual.

Chapter 3 : Installation

- Please follow the instructions below to install the SNMP IPv6.

Step 1 Remove the cover and two screws on the SNMP slot.

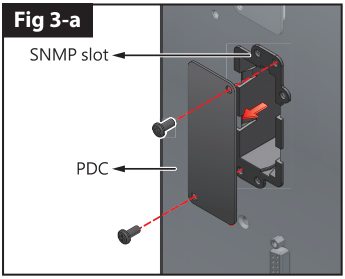


Fig 3-a

NOTE

Screw locations may vary depending on your PDC models.

Step 2 Locate the grooves on of the SNMP slot. Insert the SNMP IPv6 into the SNMP slot.

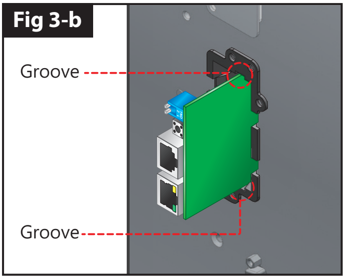


Fig 3-b

Step 3 From the accessory package, pick a cover that fits the screw locations of your PDC's SNMP slot and secure it with the removed screws.

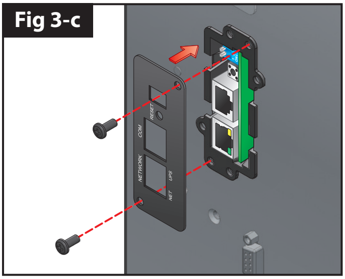


Fig 3-c

Chapter 4 : System Configurations

There are different ways you can configure your SNMP IPv6. If a network connection is available at your location, the following methods can be used:

- **Web-based interface** : The InsightPower SNMP IPv6 for PDC Web offers comprehensive system management and monitoring. Please refer to ***Chapter 5: InsightPower SNMP IPv6 for PDC Web***.
- **EzSetting** : Use the provided program EzSetting to quickly set up your SNMP IPv6. Please refer to ***4-2 Configuring with EzSetting***.
- **Telnet mode** : Configure your SNMP IPv6 in text mode. Please refer to ***4-3 Configuring via Telnet***.

The above-mentioned methods require network connection. If not available, you can use direct COM port connection to set up your SNMP IPv6. Please see ***4-4 Configuring through COM Port***.

NOTE

1. To ensure system security, it is highly recommended that you change your account and password after the first login.
2. If you have multiple SNMP IPv6 units installed in your network, we highly suggest that you change the SNMP IPv6's default Host Name to avoid conflicts. Also, it is recommended that you disable BOOTP/ DHCP and manually assign a valid static IP address to the SNMP IPv6.

4-1 Configuring via InsightPower SNMP IPv6 for PDC Web

To set up the SNMP IPv6 via your web browser, please follow the instructions below:

Step 1 Use a CAT5 network cable to connect the SNMP IPv6's Network port to the network. Launch your web browser. In the address bar, enter the SNMP IPv6's default Host Name **InsightPower**, or default IP address **192.168.1.100**. If you are unable to connect, please see ***Chapter 7 : Troubleshooting Q6***.

NOTE

If you have previously changed the SNMP IPv6's Host Name or IP address, connect with the new settings.

Step 2 Log in as Administrator (default account/ password: admin/ password, case sensitive).

Step 3 Specify your preferred display language (default: English) from the drop-down menu on the top right of the page. The SNMP IPv6 remembers your language preference. In the following instructions, English is chosen as the display language.

Step 4 Click **System** → **Administration** → **User Manager**. Manage your login accounts and passwords under the "Local Authentication" subhead. The access permission for the account types is shown as follows:

1) **Administrator :** Allowed to modify all settings.
2) **Device Manager :** Allowed to modify device-related settings.
3) **Read Only User :** Only allowed to view settings without the permission to make changes.

You can manually specify whether users are allowed to log in from other LANs. If you wish to block login attempts from external connections, select **Only in This LAN**. Otherwise, select **Allow Any**.

Step 5 Click **System** → **Administration** → **TCP/ IP** to set Host Name, IP address, Subnet Mask and Gateway IP for the SNMP IPv6.

Step 6 Click **Time Server** to manually set time and date for the system, or enable automatic time synchronization between the SNMP IPv6 and the time servers.

NOTE

To completely set up your SNMP IPv6, please refer to ***Chapter 5: InsightPower SNMP IPv6 for PDC Web***.

4-2 Configuring with EzSetting

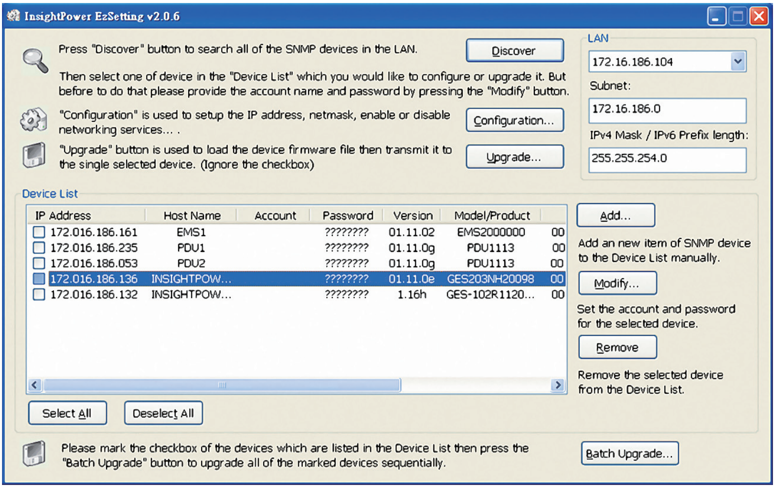
Included in the provided CD, the EzSetting (compatible with Windows 2000/ 2003/ 2008/ XP/ Vista/ 7) allows you to easily configure your SNMP IPv6 and upgrade firmware on your SNMP devices. Follow the instructions below:

Step 1 Use a CAT5 cable to connect the SNMP IPv6's Network port to the network.

Step 2 Make sure the two DIP switches of the SNMP IPv6 are set to the **OFF** position (Normal Mode) to enable network communication. Make sure the workstation and the SNMP IPv6 are on the same LAN.

Step 3 Insert the provided CD in the CD-ROM drive. From the root directory, launch EzSetting.

Step 4 Click **Discover** to search all available SNMP devices on the LAN. A list of devices will be shown.



InsightPower EzSetting v2.0.6

Press "Discover" button to search all of the SNMP devices in the LAN.

Then select one of device in the "Device List" which you would like to configure or upgrade it. But before to do that please provide the account name and password by pressing the "Modify" button.

"Configuration" is used to setup the IP address, netmask, enable or disable networking services... .

"Upgrade" button is used to load the device firmware file then transmit it to the single selected device. (Ignore the checkbox)

LAN: 172.16.186.104

Subnet: 172.16.186.0

IPv4 Mask / IPv6 Prefix length: 255.255.254.0

Device List

IP Address	Host Name	Account	Password	Version	Model/Product	
□ 172.016.186.161	EMS1		????????	01.11.02	EMS2000000	00
□ 172.016.186.235	PDU1		????????	01.11.0g	PDU1113	00
□ 172.016.186.053	PDU2		????????	01.11.0g	PDU1113	00
□ 172.016.186.136	INSIGHTPOW...		????????	01.11.0e	GES203NH20098	00
□ 172.016.186.132	INSIGHTPOW...		????????	1.16h	GES-102R1120...	00

Add an new item of SNMP device to the Device List manually.

Set the account and password for the selected device.

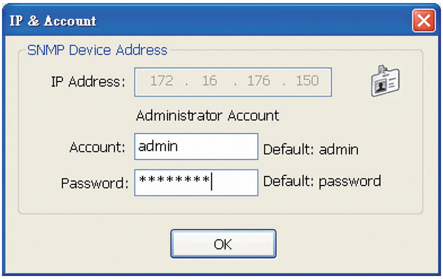
Remove the selected device from the Device List.

Please mark the checkbox of the devices which are listed in the Device List then press the "Batch Upgrade" button to upgrade all of the marked devices sequentially.

NOTE

1. If you want to search SNMP devices in a different domain, change the **Subnet** and **IPv4/ IPv6 Prefix Length** and click **Discover**.
2. If the SNMP IPv6 can not be found, check UDP port 3456 on the workstation you are using. Make sure it is open.

Step 5 Select the SNMP IPv6 that you want to modify from the Device List. Click **Modify** and enter Administrator's account and password (default: admin/ password, case sensitive).



IP & Account

SNMP Device Address

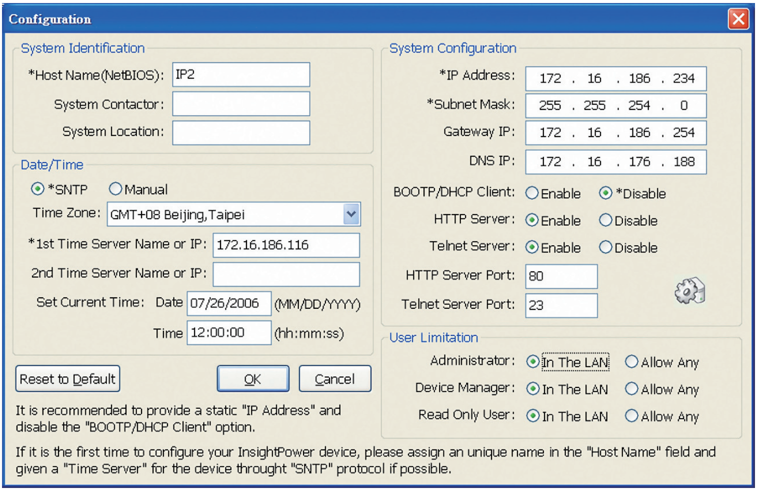
IP Address: 172 . 16 . 176 . 150

Administrator Account

Account: admin Default: admin

Password: ******** Default: password

Step 6 Click **Configuration** to configure network settings.



Configuration

System Identification

*Host Name(NetBIOS): IP2

System Contactor:

System Location:

Date/Time

● *SNTP ○ Manual

Time Zone: GMT+08 Beijing,Taipei

*1st Time Server Name or IP: 172.16.186.116

2nd Time Server Name or IP:

Set Current Time: Date 07/26/2006 (MM/DD/YYYY)

Time 12:00:00 (hh:mm:ss)

System Configuration

*IP Address: 172 . 16 . 186 . 234

*Subnet Mask: 255 . 255 . 254 . 0

Gateway IP: 172 . 16 . 186 . 254

DNS IP: 172 . 16 . 176 . 188

BOOTP/DHCP Client: ○ Enable ● *Disable

HTTP Server: ● Enable ○ Disable

Telnet Server: ● Enable ○ Disable

HTTP Server Port: 80

Telnet Server Port: 23

User Limitation

Administrator: ● In The LAN ○ Allow Any

Device Manager: ● In The LAN ○ Allow Any

Read Only User: ● In The LAN ○ Allow Any

It is recommended to provide a static "IP Address" and disable the "BOOTP/DHCP Client" option.

If it is the first time to configure your InsightPower device, please assign an unique name in the "Host Name" field and given a "Time Server" for the device throught "SNTP" protocol if possible.

NOTE

Refer to ***Chapter 5 : InsightPower SNMP IPv6 for PDC Web*** for complete configurations.

4-3 Configuring via Telnet

Step 1 Use a CAT5 network cable to connect the SNMP IPv6's Network port to the network.

Step 2 Connect the workstation (Windows or Linux) to the LAN that the SNMP IPv6 is connected to.

Step 3 For Windows, launch DOS prompt mode (**Start** → **Run** → key in **cmd** and press **Enter**). For Linux, launch Shell.

Step 4 Enter the following command: **telnet InsightPower** or **telnet IP address** to initiate telnet connection with the SNMP IPv6.

Step 5 When connection is established, enter Administrator's account and password (default: admin/ password, case sensitive). The Main Menu will appear on the screen. Please refer to ***4-5 Configuring via Text Mode*** for more information.

NOTE

1. The SNMP IPv6 terminates idle connections after 60 seconds.
2. Refer to ***Chapter 5: InsightPower SNMP IPv6 for PDC Web*** for complete configurations.

4-4 Configuring through COM Port

If a network connection is not available at your location, you can still set up the SNMP IPv6 via COM port connection. Please follow the instructions below:

NOTE

If you are running a non-Windows system, refer to your system's user manual for Telnet clients.

Step 1 Use the provided RJ45 to DB9 cable to connect the SNMP IPv6's COM port to the workstations' COM port.

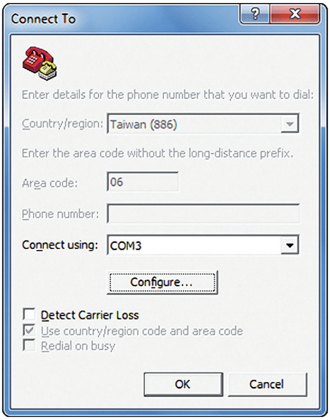
Step 2 Make sure the two DIP switches of the SNMP IPv6 are set to the **OFF** position (Normal Mode).

Step 3 For Windows 2000, 2003, 2008 and XP, go to **Start** → **Programs** → **Accessories** → **Communications** and select **HyperTerminal**.

NOTE

Microsoft has removed HyperTerminal from Windows Vista and later versions. If your operation system does not include the program, a free alternative Telnet/SSH client PuTTY can be downloaded from http://www.putty.org.

Step 4 Enter a name, choose an icon for the connection and click **OK**. From the drop-down menu **Connect using**, select the COM port that is connected to the SNMP IPv6.



Connect To

Enter details for the phone number that you want to dial:

Country/region: Taiwan (886)

Enter the area code without the long-distance prefix.

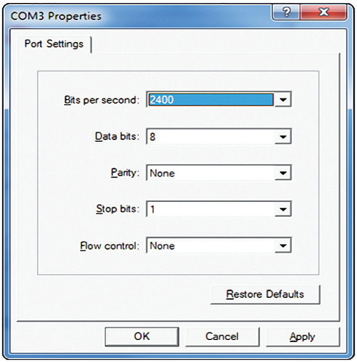
Area code: 06

Phone number:

Connect using: COM3

☐ Detect Carrier Loss
☑ Use country/region code and area code
☐ Redial on busy

Step 5 Click **Configure** and set up COM port parameters as follows:


COM3 Properties

Port Settings

Bits per second: 2400

Data bits: 8

Parity: None

Stop bits: 1

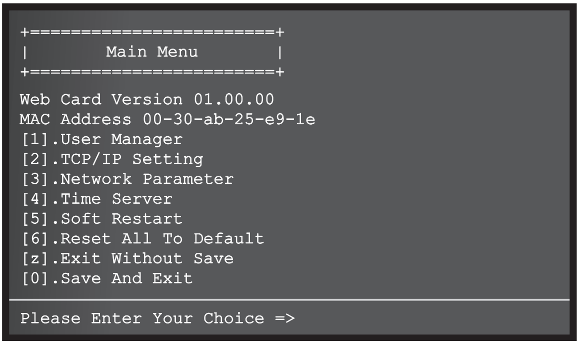
Flow control: None

Step 6 Click **OK** to continue. Set the two DIP switches of the SNMP IPv6 to the **ON** position (Configuration Mode), and HyperTerminal will automatically connect to the SNMP IPv6. If it does not connect, click the telephone icon from the tool bar. When connection is established, log in with Administrator's account/ password (default: admin/ password, case sensitive). Once you are logged in, the Main Menu appears on the screen. Please refer to ***4-5 Configuring via Text Mode*** for more information.

4-5 Configuring via Text Mode

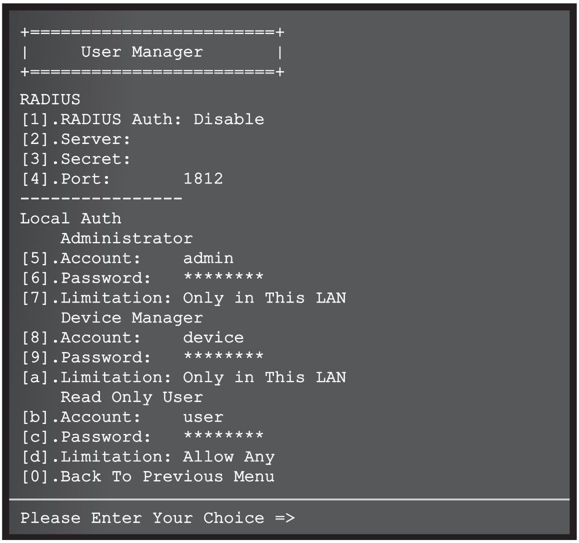
You can configure the SNMP IPv6 via text mode by using Telnet/ SSH clients such as HyperTerminal and PuTTY. In this section, you can find descriptions and default settings.

Main Menu



```
+========================+
|        Main Menu       |
+========================+
Web Card Version 01.00.00
MAC Address 00-30-ab-25-e9-1e
[1].User Manager
[2].TCP/IP Setting
[3].Network Parameter
[4].Time Server
[5].Soft Restart
[6].Reset All To Default
[z].Exit Without Save
[0].Save And Exit

Please Enter Your Choice =>
```

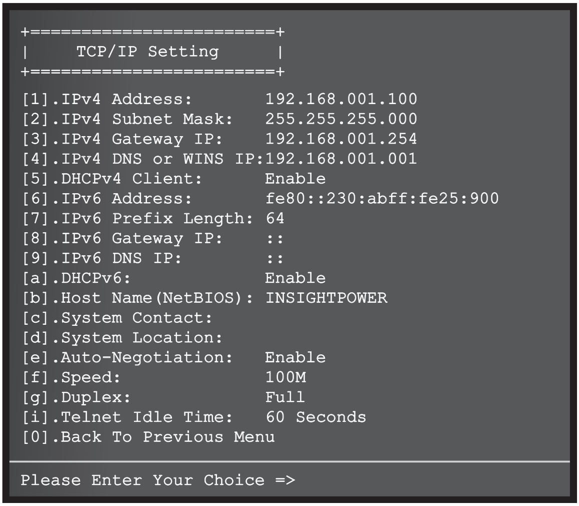
User Manager



```
+========================+
|      User Manager      |
+========================+
RADIUS
[1].RADIUS Auth: Disable
[2].Server:
[3].Secret:
[4].Port:        1812
----------------
Local Auth
    Administrator
[5].Account:     admin
[6].Password:    ********
[7].Limitation: Only in This LAN
    Device Manager
[8].Account:     device
[9].Password:    ********
[a].Limitation: Only in This LAN
    Read Only User
[b].Account:     user
[c].Password:    ********
[d].Limitation: Allow Any
[0].Back To Previous Menu

Please Enter Your Choice =>
```

No.	Item	Description	Default
[1]	RADIUS Auth	Specify whether RADIUS login is allowed.	Disable
[2]	Server	The RADIUS server name.	
[3]	Secret	The RADIUS secret.	
[4]	Port	The RADIUS port.	1812
[5]	Administrator Account	The default account/ password for the Administrator (case sensitive).	admin
[6]	Administrator Password		password
[7]	Administrator Limitation	Restrict Administrator login area.	Only in This LAN
[8]	Device Manager Account	The default account/ password (case sensitive) for the Device Manager. This account is only permitted to change device-related settings.	device
[9]	Device Manager Password		password
[a]	Device Manager Limitation	Restrict Device Manager login area.	Only in This LAN
[b]	Read Only User Account	The default account/ password (case sensitive) for Read Only User. This account is only allowed to view settings without the permission to make changes.	user
[c]	Read Only User Password		password
[d]	Read Only User Limitation	Restrict Read Only User login area.	Allow Any

TCP/IP Setting

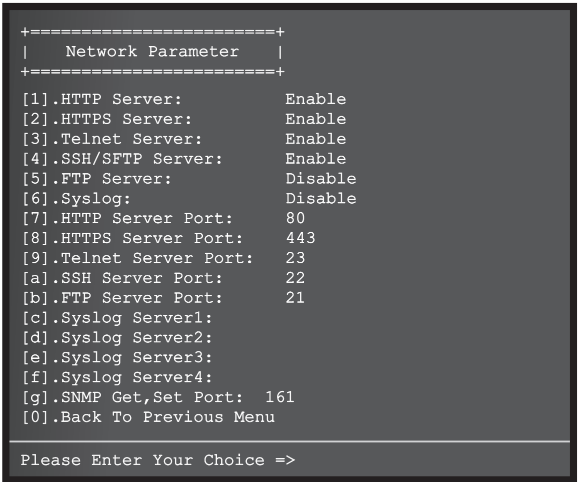


```
+========================+
|     TCP/IP Setting     |
+========================+
[1].IPv4 Address:       192.168.001.100
[2].IPv4 Subnet Mask:   255.255.255.000
[3].IPv4 Gateway IP:    192.168.001.254
[4].IPv4 DNS or WINS IP:192.168.001.001
[5].DHCPv4 Client:      Enable
[6].IPv6 Address:       fe80::230:abff:fe25:900
[7].IPv6 Prefix Length: 64
[8].IPv6 Gateway IP:    ::
[9].IPv6 DNS IP:        ::
[a].DHCPv6:             Enable
[b].Host Name(NetBIOS): INSIGHTPOWER
[c].System Contact:
[d].System Location:
[e].Auto-Negotiation:   Enable
[f].Speed:              100M
[g].Duplex:             Full
[i].Telnet Idle Time:   60 Seconds
[0].Back To Previous Menu

Please Enter Your Choice =>
```

No.	Item	Description	Default
[1]	IPv4 Address	The IPv4 address.	192.168.001.100
[2]	IPv4 Subnet Mask	The IPv4 subnet mask setting.	255.255.255.000
[3]	IPv4 Gateway IP	The IPv4 gateway's IP address.	192.168.001.254
[4]	IPv4 DNS or WINS IP	IPv4 Domain Name Server or WINS IP.	192.168.001.001
[5]	DHCPv4 Client	Enable/ disable DHCPv4 protocol.	Enable
[6]	IPv6 Address	The IPv6 address.	
[7]	IPv6 Prefix Length	The IPv6 prefix length.	
[8]	IPv6 Gateway IP	The IPv6 gateway's IP address.	
[9]	IPv6 DNS IP	IPv6 Domain Name Server's IP address.	
[a]	DHCPv6	Enable/ disable DHCPv6 protocol.	Enable
[b]	Host Name (NetBIOS)	The Host Name for the SNMP IPv6.	INSIGHTPOWER

No.	Item	Description	Default
[c]	System Contact	The System Contact information.	
[d]	System Location	The System Location information.	
[e]	Auto-Negotiation	Enable/disable automatic transfer rate (10/ 100Mbps) negotiation.	Enable
[f]	Speed	If the Auto-Negotiation is disabled, you can specify the transfer rate.	100M
[g]	Duplex	If the Auto-Negotiation is disabled, you can specify the duplex mode.	Full
[i]	Telnet Idle Time	Telnet connection time-out setting.	60 Seconds

Network Parameter

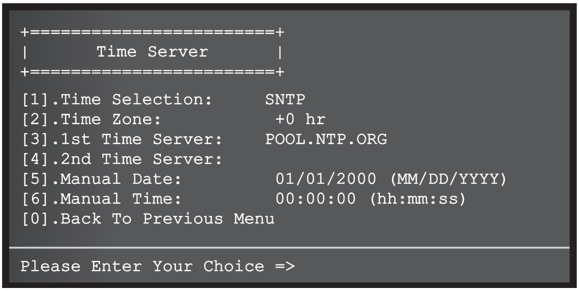


```
+========================+
|    Network Parameter    |
+========================+
[1].HTTP Server:          Enable
[2].HTTPS Server:         Enable
[3].Telnet Server:        Enable
[4].SSH/SFTP Server:      Enable
[5].FTP Server:           Disable
[6].Syslog:               Disable
[7].HTTP Server Port:     80
[8].HTTPS Server Port:    443
[9].Telnet Server Port:   23
[a].SSH Server Port:      22
[b].FTP Server Port:      21
[c].Syslog Server1:
[d].Syslog Server2:
[e].Syslog Server3:
[f].Syslog Server4:
[g].SNMP Get,Set Port:  161
[0].Back To Previous Menu

Please Enter Your Choice =>
```

No.	Item	Description	Default
[1]	HTTP Server	Enable/ disable HTTP protocol.	Enable
[2]	HTTPS Server	Enable/ disable HTTPS protocol.	Enable
[3]	Telnet Server	Enable/ disable Telnet protocol.	Enable
[4]	SSH/ SFTP Server	Enable/ disable SSH/ SFTP protocol.	Enable
[5]	FTP Server	Enable/ disable FTP protocol.	Disable
[6]	Syslog	Enable/ disable remote Syslog.	Disable
[7]	HTTP Server Port	HTTP port.	80
[8]	HTTPS Server Port	HTTPS port.	443
[9]	Telnet Server Port	Telnet port.	23
[a]	SSH Server Port	SSH port.	22
[b]	FTP Server Port	FTP port.	21
[c]	Syslog Server 1	The Host Name of remote Syslog Server 1.	
[d]	Syslog Server 2	The Host Name of remote Syslog Server 2.	
[e]	Syslog Server 3	The Host Name of remote Syslog Server 3.	
[f]	Syslog Server 4	The Host Name of remote Syslog Server 4.	
[g]	SNMP Get, Set Port	The SNMP port.	161

Time Server

You can manually adjust time and date for the SNMP IPv6 or set up automatic time server synchronization. The SNMP IPv6, Windows XP and later versions support SNTP (Simple Network Time Protocol). If you need to start up a time server service on your workstation, please refer to ***Chapter 7: Troubleshooting Q1***.



```
+========================+
|      Time Server       |
+========================+
[1].Time Selection:     SNTP
[2].Time Zone:           +0 hr
[3].1st Time Server:    POOL.NTP.ORG
[4].2nd Time Server:
[5].Manual Date:         01/01/2000 (MM/DD/YYYY)
[6].Manual Time:         00:00:00 (hh:mm:ss)
[0].Back To Previous Menu

Please Enter Your Choice =>
```

No.	Item	Description	Default
[1]	Time Selection	SNTP or manual.	SNTP
[2]	Time Zone	Adjust your time zone.	+0 hr
[3]	1st Time Server	The first time server for SNTP.	POOL.NTP.ORG
[4]	2nd Time Server	The second time server for SNTP.	
[5]	Manual Date	Set the date manually.	01/01/2000
[6]	Manual Time	Set the time manually.	00:00:00

Soft Restart

Reset the SNMP IPv6. This will not affect the operation of the PDC.

Default Reset

Reset to manufacture default.

Exit Without Saving

Exit and ignore changes.

Save and Exit

Preserve your changes and exit.

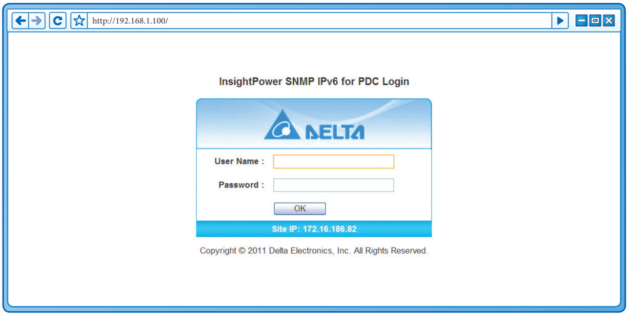
Chapter 5 : InsightPower SNMP IPv6 for PDC Web

To configure the SNMP IPv6 via the InsightPower SNMP IPv6 for PDC Web, please follow the steps below:

Step 1 Make sure that your SNMP IPv6 is connected to the LAN. Use a CAT5 network cable to connect the SNMP IPv6's Network port to the network.

Step 2 Launch your web browser. In the address bar, enter the SNMP IPv6's Host Name **http:/InsightPower/** or **IP address**. For encrypted connection, enter **https://InsightPower/** or **https://192.168.1.100/**.

Step 3 When connection is established, the login page appears. Enter your account and password (default: admin/ password).



http://192.168.1.100/

InsightPower SNMP IPv6 for PDC Login

Site IP: 172.16.186.82

Copyright © 2011 Delta Electronics, Inc. All Rights Reserved.

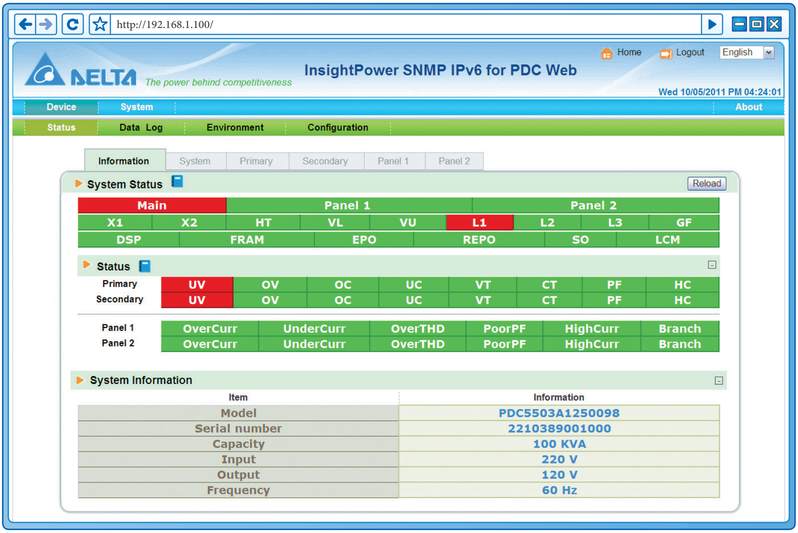
NOTE

1. If you have previously changed the SNMP IPv6's Host Name or IP address, please connect with new settings.
2. If the login page is accessible, but you are unable to log in with correct account and password, additional network configuration may be needed. The cause could be the IP subnet of the computer you are logging in to is different from the SNMP IPv6's. To solve this issue, please refer to ***Chapter 7: Troubleshooting Q3***.
3. The SNMP IPv6 will automatically log off idle connections after 30 minutes.

5-1 Device

In this page, check PDC's system status and readings. This page automatically refreshes every 10 seconds. Click **Reload** to manually refresh. A slide-in window shows to provide additional information when you click on the 📘 icon. Click **Close** the slide-in window will disappear.

To change a setting, select from the drop-down menu or simply click on the item. Input new value in the text box and click **Submit** to take effect.



System Status

Main	Panel 1				Panel 2			
X1	X2	HT	VL	VU	L1	L2	L3	GF

DSP	FRAM	EPO	REPO	SO	LCM

Status

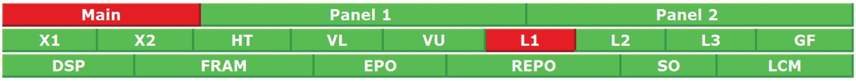
Primary	UV	OV	OC	UC	VT	CT	PF	HC
Secondary	UV	OV	OC	UC	VT	CT	PF	HC

Panel 1	OverCurr	UnderCurr	OverTHD	PoorPF	HighCurr	Branch
Panel 2	OverCurr	UnderCurr	OverTHD	PoorPF	HighCurr	Branch

System Information

Item	Information
Model	PDC5503A1250098
Serial number	2210389001000
Capacity	100 KVA
Input	220 V
Output	120 V
Frequency	60 Hz

5-1-1 Status



Main | Panel 1 | Panel 2

X1 | X2 | HT | VL | VU | L1 | L2 | L3 | GF

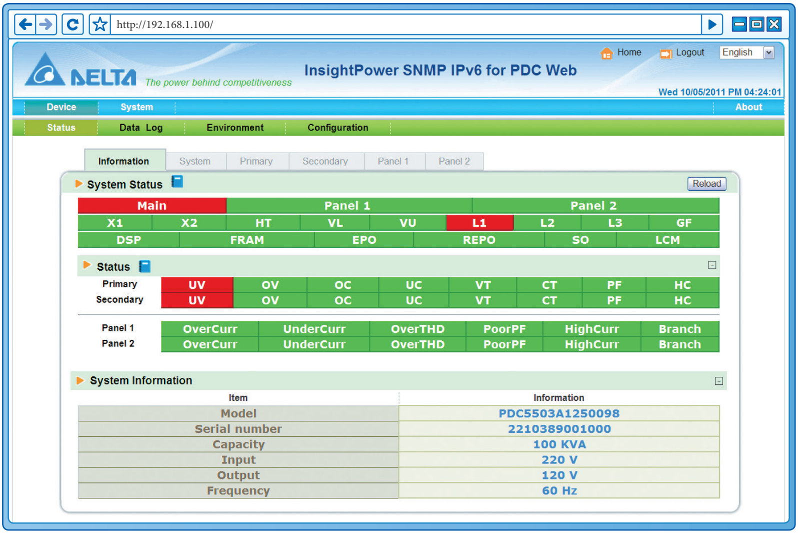
DSP | FRAM | EPO | REPO | SO | LCM

The red and green flags represent the PDC's status. A green flag shows to indicate normal operation. A red flag means a warning event has occurred. Refer to the following table for flags and the warning events they represent:

Flag	Description	Flag	Description
Main	A warning event of the main breaker has occurred.	**Panel #**	A warning event of the panel breaker has occurred.
X1/ X2	X1 : Transformer temperature exceeds 125 c. X2 : Transformer temperature exceeds 150 c.	**HT**	Ambient temperature too high.
VL	Voltage phase lacking.	**VU**	Voltage unbalance.
L1/ L2/ L3	Frequency out of range.	**GF**	Ground fault.
DSP	CAN DSP communication error.	**FRAM**	FRAM read/ write error.
EPO	Emergency Power Off initiated.	**REPO**	Remote Emergency Power Off initiated.
SO	System overload.	**LCM**	CAN LCM communication error.
UV	Under voltage.	**OV**	Over voltage.
OC	Over current.	**UC**	Under current.
VT	Over voltage THD.	**CT**	Over current THD.
PF	Poor power factor.	**HC**	High current.

Information

This page shows a quick review of PDC's status and system information, including model, serial number, capacity, input/ output voltage and frequency.



System Status

Main		Panel 1			Panel 2			
X1	X2	HT	VL	VU	L1	L2	L3	GF

DSP	FRAM	EPO	REPO	SO	LCM

Status

Primary	UV	OV	OC	UC	VT	CT	PF	HC
Secondary	UV	OV	OC	UC	VT	CT	PF	HC

Panel 1	OverCurr	UnderCurr	OverTHD	PoorPF	HighCurr	Branch
Panel 2	OverCurr	UnderCurr	OverTHD	PoorPF	HighCurr	Branch

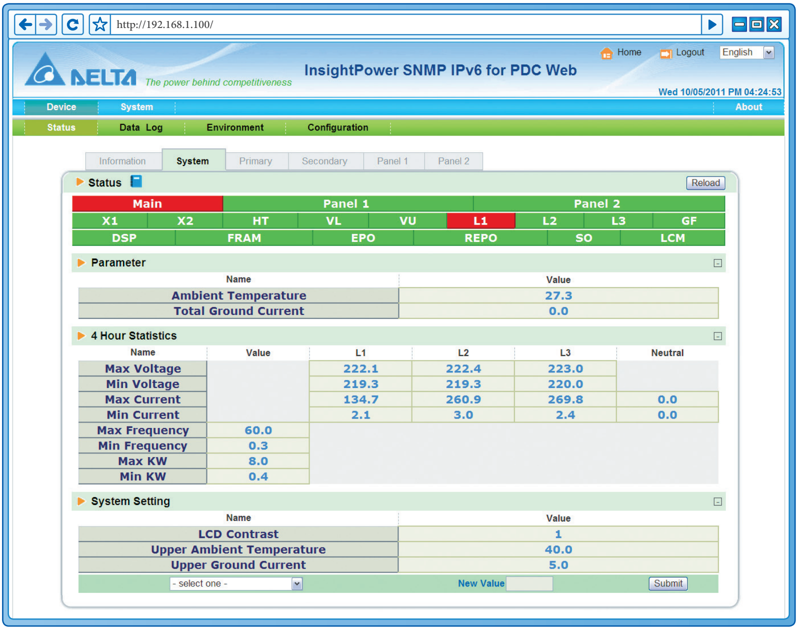
System Information

Item	Information
Model	PDC5503A1250098
Serial number	2210389001000
Capacity	100 KVA
Input	220 V
Output	120 V
Frequency	60 Hz

System

In this page, check PDC’s status, , statistics and settings. 4 Hour Statistics shows circuit readings that are recorded during the past four hours.

To change a setting, simply click on it, or select from the drop-down menu on the bottom of the page. Make sure to click **Submit** to take effect after the changes are made.



Status

Main	Panel 1				Panel 2			
X1	X2	HT	VL	VU	L1	L2	L3	GF
DSP	FRAM	EPO	REPO	SO	LCM			

Parameter

Name	Value
Ambient Temperature	27.3
Total Ground Current	0.0

4 Hour Statistics

Name	Value	L1	L2	L3	Neutral
Max Voltage		222.1	222.4	223.0	
Min Voltage		219.3	219.3	220.0	
Max Current		134.7	260.9	269.8	0.0
Min Current		2.1	3.0	2.4	0.0
Max Frequency	60.0				
Min Frequency	0.3				
Max KW	8.0				
Min KW	0.4				

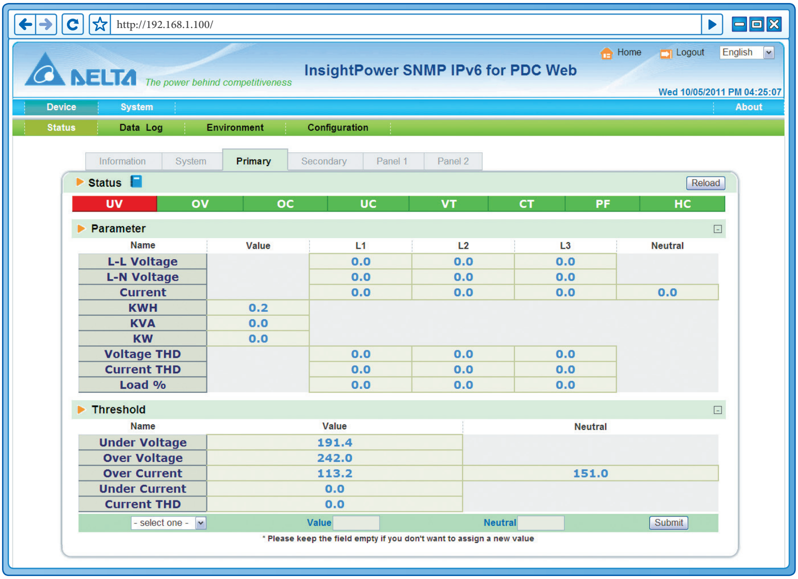
System Setting

Name	Value
LCD Contrast	1
Upper Ambient Temperature	40.0
Upper Ground Current	5.0

- select one - New Value Submit

Primary

This page shows the PDC's input readings and settings. You can change the threshold settings on the bottom of the page.



Parameter

Name	Value	L1	L2	L3	Neutral
L-L Voltage		0.0	0.0	0.0	
L-N Voltage		0.0	0.0	0.0	
Current		0.0	0.0	0.0	0.0
KWH	0.2				
KVA	0.0				
KW	0.0				
Voltage THD		0.0	0.0	0.0	
Current THD		0.0	0.0	0.0	
Load %		0.0	0.0	0.0	

Threshold

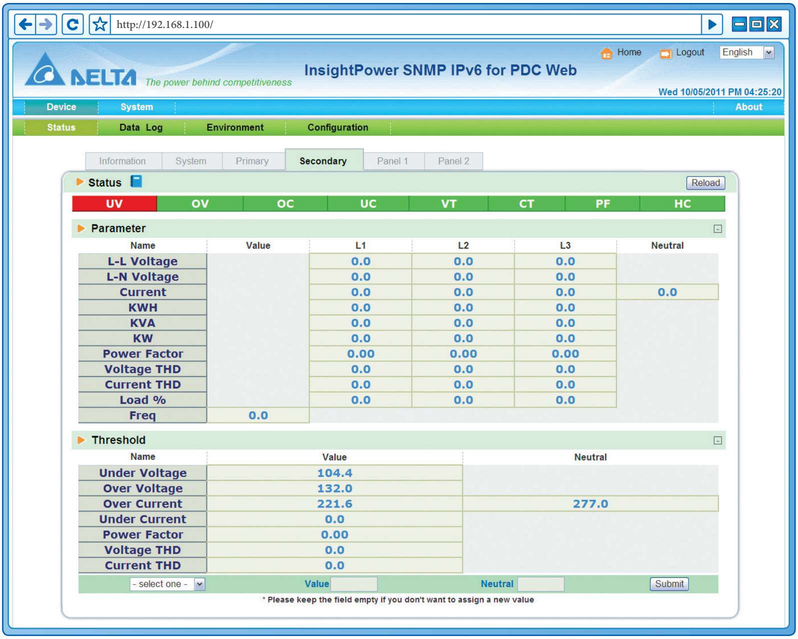
Name	Value	Neutral
Under Voltage	191.4	
Over Voltage	242.0	
Over Current	113.2	151.0
Under Current	0.0	
Current THD	0.0	

Value Neutral

* Please keep the field empty if you don't want to assign a new value

Secondary

This page shows the PDC's output readings and settings. You can change the threshold settings on the bottom of the page.



Parameter

Name	Value	L1	L2	L3	Neutral
L-L Voltage		0.0	0.0	0.0	
L-N Voltage		0.0	0.0	0.0	
Current		0.0	0.0	0.0	0.0
KWH		0.0	0.0	0.0	
KVA		0.0	0.0	0.0	
KW		0.0	0.0	0.0	
Power Factor		0.00	0.00	0.00	
Voltage THD		0.0	0.0	0.0	
Current THD		0.0	0.0	0.0	
Load %		0.0	0.0	0.0	
Freq	0.0				

Threshold

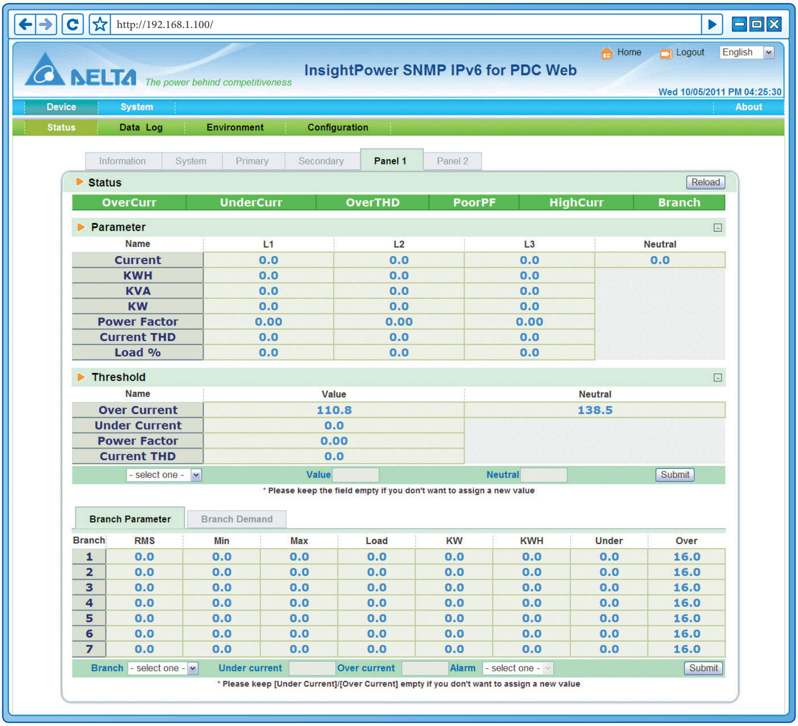
Name	Value	Neutral
Under Voltage	104.4	
Over Voltage	132.0	
Over Current	221.6	277.0
Under Current	0.0	
Power Factor	0.00	
Voltage THD	0.0	
Current THD	0.0	

- select one - Value ______ Neutral ______ Submit

* Please keep the field empty if you don't want to assign a new value

Panel

The number of panels and branch circuits may vary depending on your PDC's configurations. Check panel's readings and status in this page. To change a setting, simply click on it, or select from the drop-down menu on the bottom of the page. Make sure to click **Submit** to take effect after the changes are made.



InsightPower SNMP IPv6 for PDC Web

Wed 10/05/2011 PM 04:25:30

Status

OverCurr	UnderCurr	OverTHD	PoorPF	HighCurr	Branch

Parameter

Name	L1	L2	L3	Neutral
Current	0.0	0.0	0.0	0.0
KWH	0.0	0.0	0.0	
KVA	0.0	0.0	0.0	
KW	0.0	0.0	0.0	
Power Factor	0.00	0.00	0.00	
Current THD	0.0	0.0	0.0	
Load %	0.0	0.0	0.0	

Threshold

Name	Value	Neutral
Over Current	110.8	138.5
Under Current	0.0	
Power Factor	0.00	
Current THD	0.0	

- select one - Value Neutral Submit

* Please keep the field empty if you don't want to assign a new value

Branch Parameter | Branch Demand

Branch	RMS	Min	Max	Load	KW	KWH	Under	Over
1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	16.0
2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	16.0
3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	16.0
4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	16.0
5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	16.0
6	0.0	0.0	0.0	0.0	0.0	0.0	0.0	16.0
7	0.0	0.0	0.0	0.0	0.0	0.0	0.0	16.0

Branch - select one - Under current Over current Alarm - select one - Submit

* Please keep [Under Current]/[Over Current] empty if you don't want to assign a new value

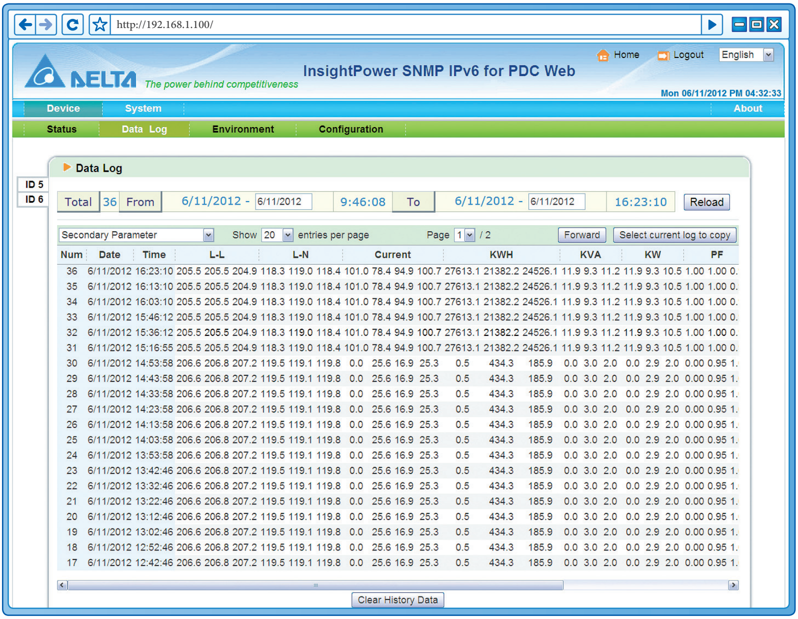
5-1-2 Data Log

Hover your cursor on a reading to check detailed information. The total number of log entries is shown on the top left of the page.

You can define a time period to show entries recorded during the specified time. Click on the date to bring up a pop-up window and specify a date. Click **Clear History Data** to clear all stored entries (for all ID tags).

To check a specific type of data entry, select a type from the drop-down menu, specify how many entries to show per page, and click **Reload**.

Click **Forward/ Backward** to select the display order of listed data logs. To copy all data entries to an Excel spreadsheet, click **Select current log to copy**. Press **CTRL + C** to copy. Press **CTRL + V** to paste in Excel.



Data Log

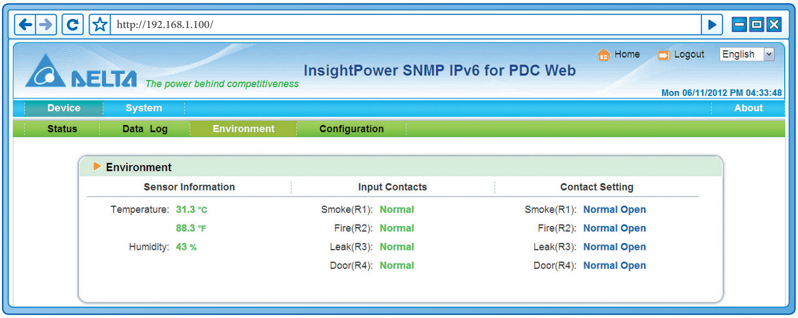
Total 36 From 6/11/2012 - 6/11/2012 9:46:08 To 6/11/2012 - 6/11/2012 16:23:10

Secondary Parameter Show 20 entries per page Page 1 / 2

Num	Date	Time	L-L			L-N			Current				KWH			KVA			KW			PF		
36	6/11/2012	16:23:10	205.5	205.5	204.9	118.3	119.0	118.4	101.0	78.4	94.9	100.7	27613.1	21382.2	24526.1	11.9	9.3	11.2	11.9	9.3	10.5	1.00	1.00	0.
35	6/11/2012	16:13:10	205.5	205.5	204.9	118.3	119.0	118.4	101.0	78.4	94.9	100.7	27613.1	21382.2	24526.1	11.9	9.3	11.2	11.9	9.3	10.5	1.00	1.00	0.
34	6/11/2012	16:03:10	205.5	205.5	204.9	118.3	119.0	118.4	101.0	78.4	94.9	100.7	27613.1	21382.2	24526.1	11.9	9.3	11.2	11.9	9.3	10.5	1.00	1.00	0.
33	6/11/2012	15:46:12	205.5	205.5	204.9	118.3	119.0	118.4	101.0	78.4	94.9	100.7	27613.1	21382.2	24526.1	11.9	9.3	11.2	11.9	9.3	10.5	1.00	1.00	0.
32	6/11/2012	15:36:12	205.5	205.5	204.9	118.3	119.0	118.4	101.0	78.4	94.9	100.7	27613.1	21382.2	24526.1	11.9	9.3	11.2	11.9	9.3	10.5	1.00	1.00	0.
31	6/11/2012	15:16:55	205.5	205.5	204.9	118.3	119.0	118.4	101.0	78.4	94.9	100.7	27613.1	21382.2	24526.1	11.9	9.3	11.2	11.9	9.3	10.5	1.00	1.00	0.
30	6/11/2012	14:53:58	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.
29	6/11/2012	14:43:58	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.
28	6/11/2012	14:33:58	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.
27	6/11/2012	14:23:58	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.
26	6/11/2012	14:13:58	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.
25	6/11/2012	14:03:58	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.
24	6/11/2012	13:53:58	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.
23	6/11/2012	13:42:46	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.
22	6/11/2012	13:32:46	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.
21	6/11/2012	13:22:46	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.
20	6/11/2012	13:12:46	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.
19	6/11/2012	13:02:46	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.
18	6/11/2012	12:52:46	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.
17	6/11/2012	12:42:46	206.6	206.8	207.2	119.5	119.1	119.8	0.0	25.6	16.9	25.3	0.5	434.3	185.9	0.0	3.0	2.0	0.0	2.9	2.0	0.00	0.95	1.

5-1-3 Environment

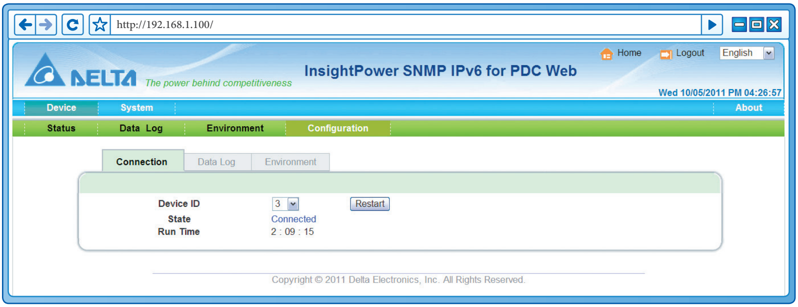
This page only appears when an EnviroProbe is connected. You can check the temperature/ humidity readings and the status of input contacts.



Environment

Sensor Information		Input Contacts		Contact Setting	
Temperature:	31.3 °C	Smoke(R1):	Normal	Smoke(R1):	Normal Open
	88.3 °F	Fire(R2):	Normal	Fire(R2):	Normal Open
Humidity:	43 %	Leak(R3):	Normal	Leak(R3):	Normal Open
		Door(R4):	Normal	Door(R4):	Normal Open

5-1-4 Configuration


http://192.168.1.100/
Home
Logout
English
DELTA
The power behind competitiveness
InsightPower SNMP IPv6 for PDC Web
Wed 10/05/2011 PM 04:26:57
Device
System
About
Status
Data Log
Environment
Configuration
Connection
Data Log
Environment
Restart
Copyright © 2011 Delta Electronics, Inc. All Rights Reserved.

Device ID 3
State Connected
Run Time 2 : 09 : 15

Connection

By default, the PDC has a device ID of 1, which also represents the ID assigned in Modbus protocol. To link the PDC with the SNMP IPv6, the device ID setting must match. Select the PDC's device ID and click **Restart**.

Data Log

Specify the data saving frequency for the Data Log. The system automatically saves data after the specified time elapses. Click **Apply** to take effect.

Environment

This page only appears when an EnviroProbe is connected. Set warning and alarm thresholds. Entitle input contacts and select their contact types respectively. Click **Submit** to take effect.

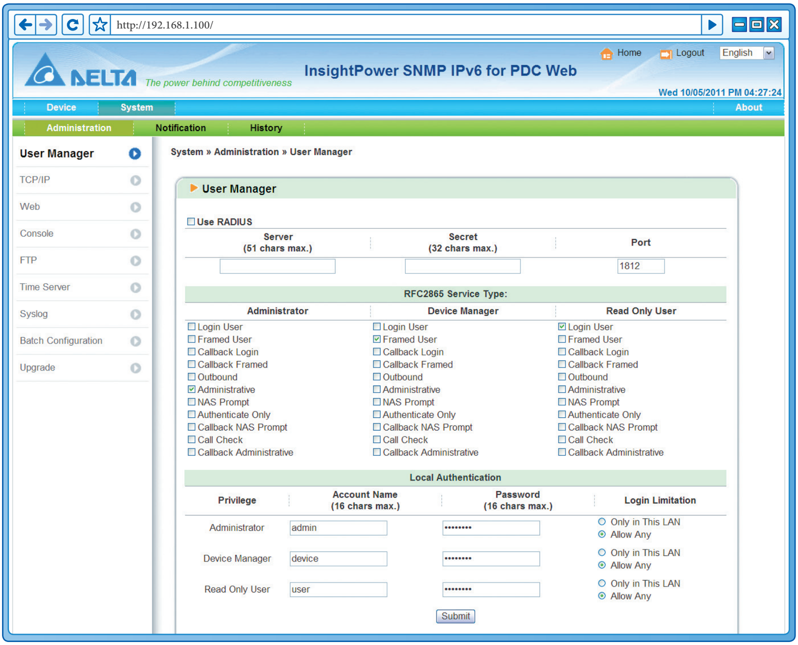
5-2 System

Check or change system configurations in the following pages.

5-2-1 Administration

User Manager

The SNMP IPv6 supports RADIUS. Specify server, secret and port (default: 1812). Check **User RADIUS** and click **Submit** to activate. Check specific service types for Administrator, Device Manager and Read Only User. If RADIUS is disabled, local authentication will be used. Specify account name, password and login limitation for individual accounts.



User Manager

□ Use RADIUS

Server (51 chars max.)	Secret (32 chars max.)	Port
		1812

RFC2865 Service Type:

Administrator	Device Manager	Read Only User
□ Login User	□ Login User	☑ Login User
□ Framed User	☑ Framed User	□ Framed User
□ Callback Login	□ Callback Login	□ Callback Login
□ Callback Framed	□ Callback Framed	□ Callback Framed
□ Outbound	□ Outbound	□ Outbound
☑ Administrative	□ Administrative	□ Administrative
□ NAS Prompt	□ NAS Prompt	□ NAS Prompt
□ Authenticate Only	□ Authenticate Only	□ Authenticate Only
□ Callback NAS Prompt	□ Callback NAS Prompt	□ Callback NAS Prompt
□ Call Check	□ Call Check	□ Call Check
□ Callback Administrative	□ Callback Administrative	□ Callback Administrative

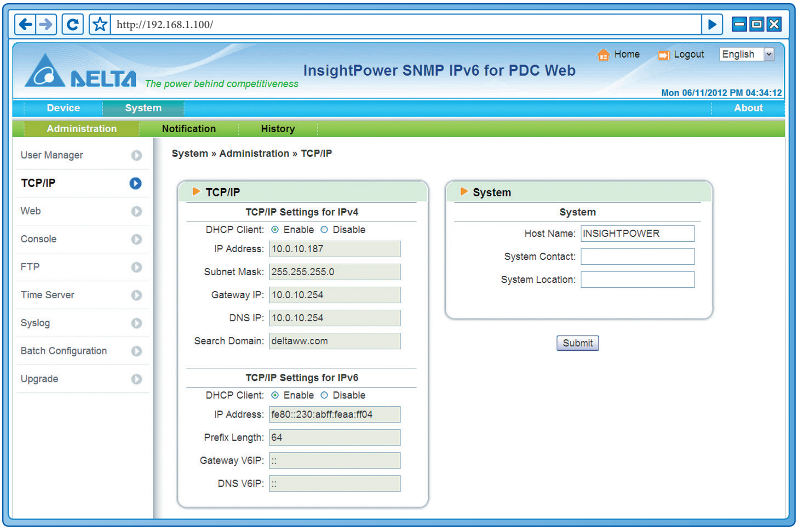
Local Authentication

Privilege	Account Name (16 chars max.)	Password (16 chars max.)	Login Limitation
Administrator	admin	••••••••	○ Only in This LAN ● Allow Any
Device Manager	device	••••••••	○ Only in This LAN ● Allow Any
Read Only User	user	••••••••	○ Only in This LAN ● Allow Any

Submit

TCP/ IP

Set up TCP/ IP protocol settings in this page.



System » Administration » TCP/IP

TCP/IP

TCP/IP Settings for IPv4

DHCP Client: ● Enable ○ Disable

IP Address: 10.0.10.187

Subnet Mask: 255.255.255.0

Gateway IP: 10.0.10.254

DNS IP: 10.0.10.254

Search Domain: deltaww.com

TCP/IP Settings for IPv6

DHCP Client: ● Enable ○ Disable

IP Address: fe80::230:abff:feaa:ff04

Prefix Length: 64

Gateway V6IP: ::

DNS V6IP: ::

System

System

Host Name: INSIGHTPOWER

System Contact:

System Location:

- **IPv4 TCP/ IP Settings for IPv4**

  Specify IPv4 IP address, subnet mask, gateway IP, DNS IP and search domain. If IPv4 DHCP is enabled, the DHCP server automatically assigns an IP address to the SNMP IPv6. If the Host Name you provided cannot be found, the system appends the search domain to your Host Name.

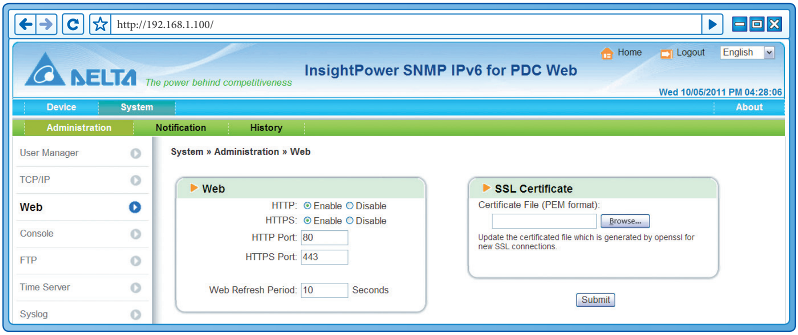
- **IPv4 TCP/ IP Settings for IPv6**

  Specify IPv6 IP address, subnet mask, gateway IP, DNS IP and search domain. If IPv6 DHCP is enabled, the DHCP server automatically assigns an IP address to the SNMP IPv6. If the Host Name you provided cannot be found, the system appends the search domain to your Host Name.

- **System**

  Specify the SNMP IPv6's Host Name on the network. Provide additional information for system contact and location, which are left blank by default.

Web



Web

HTTP: ⦿ Enable ○ Disable

HTTPS: ⦿ Enable ○ Disable

HTTP Port: 80

HTTPS Port: 443

Web Refresh Period: 10 Seconds

SSL Certificate

Certificate File (PEM format):

Update the certificated file which is generated by openssl for new SSL connections.

- **Web**

  Enable/ disable HTTP/ HTTPS protocols. Change default ports (HTTP : 80, HTTPS : 443). Specify the web refresh period (default: 10 seconds). The Device → Status and Environment pages automatically refresh and update the provided information after the specified time elapses.

- **SSL Certificate**

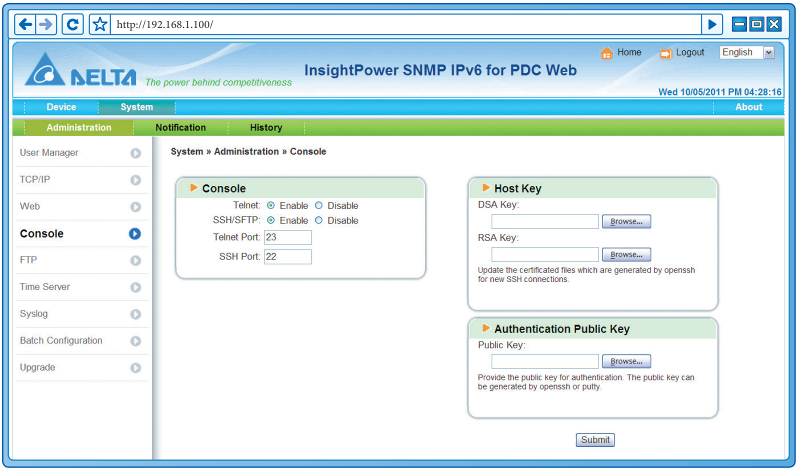
  SSL Certificate can be used to encrypt data to improve connect security. The SNMP IPv6 supports PEM format generated by OpenSSL. Click **Browse** to upload a certificate file.

NOTE

For more information regarding generating a private SSL certificate file, please refer to ***Chapter 7: Troubleshooting Q12***, or visit http://www.openssl.org/.

Console

This page allows you to enable or disable Telnet/ SSH communication protocols and replace DSA/ RSA keys.



Console

Telnet: ● Enable ○ Disable

SSH/SFTP: ● Enable ○ Disable

Telnet Port: 23

SSH Port: 22

Host Key

DSA Key:

RSA Key:

Update the certificated files which are generated by openssh for new SSH connections.

Authentication Public Key

Public Key:

Provide the public key for authentication. The public key can be generated by openssh or putty.

- **Console**

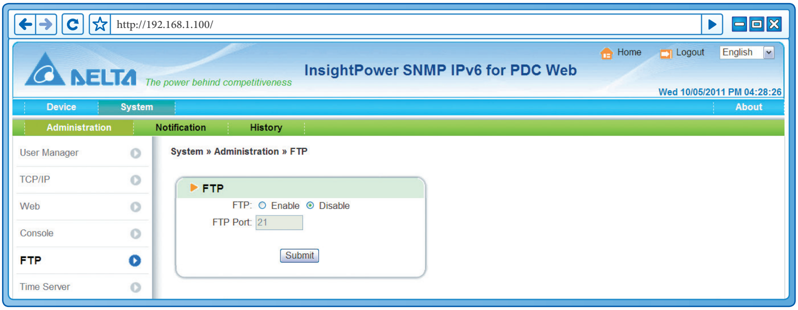
  Enable/ disable Telnet and SSH/FTP protocols. Assign ports when used.

- **Host Key**

  The SNMP IPv6 supports SSH encryption to secure data communication. Refer to ***Chapter 7: Troubleshooting Q13*** to generate DSA, RSA and public keys. The keys can be uploaded via this page or via SFTP protocol. To upload your keys, refer to ***Chapter 7: Troubleshooting Q14***.

FTP

Enable/ disable FTP protocol. Assign a port when used.



System » Administration » FTP

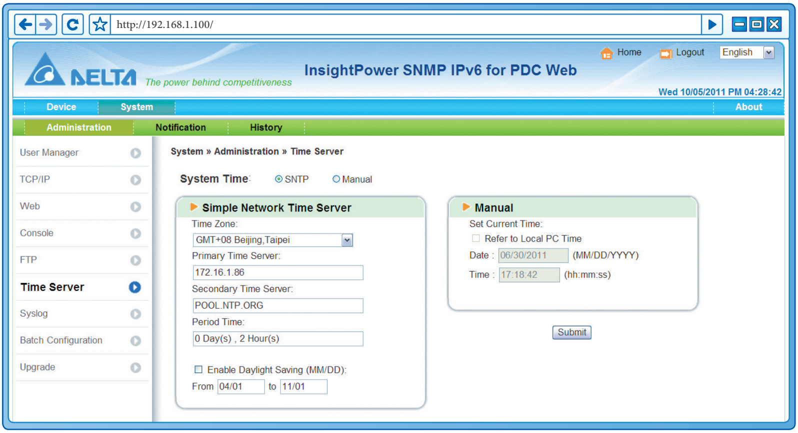
FTP

FTP: ○ Enable ● Disable

FTP Port: 21

Time Server

You can manually set the time and date, or enable automatic time synchronization with SNTP servers. Please note that if the assigned SNTP server is not responsive, the event and data log will not be recorded even when the SNTP is enabled.



System » Administration » Time Server

System Time: ● SNTP ○ Manual

Simple Network Time Server

Time Zone: GMT+08 Beijing,Taipei

Primary Time Server: 172.16.1.86

Secondary Time Server: POOL.NTP.ORG

Period Time: 0 Day(s) , 2 Hour(s)

□ Enable Daylight Saving (MM/DD):

From 04/01 to 11/01

Manual

Set Current Time:

□ Refer to Local PC Time

Date : 06/30/2011 (MM/DD/YYYY)

Time : 17:18:42 (hh:mm:ss)

Simple Network Time Server

From the dropdown menu, select the time zone for the location where the SNMP IPv6 is located. Specify the IP addresses or domain names for the primary and secondary time servers. The SNMP IPv6 synchronizes with the first responding server based on the frequency you specified.

If daylight saving is enabled, during the assigned period, the SNMP IPv6 adjusts forward one hour.

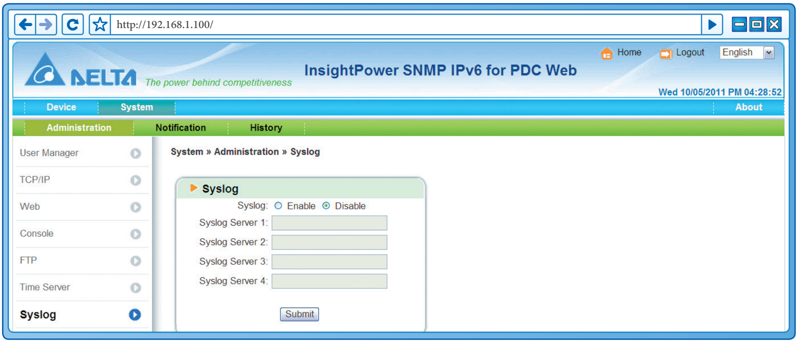
- **Manual**

  If a time server is not accessible, you can still manually set time and date.

  Please note that every time you restart the SNMP IPv6, time and date is reinstated to previous assigned settings.

Syslog

Syslog is used to store event logs on remote syslog servers. This will not affect the local event logs. Up to four syslog servers can be assigned.



System » Administration » Syslog

Syslog

Syslog: ○ Enable ● Disable

Syslog Server 1:

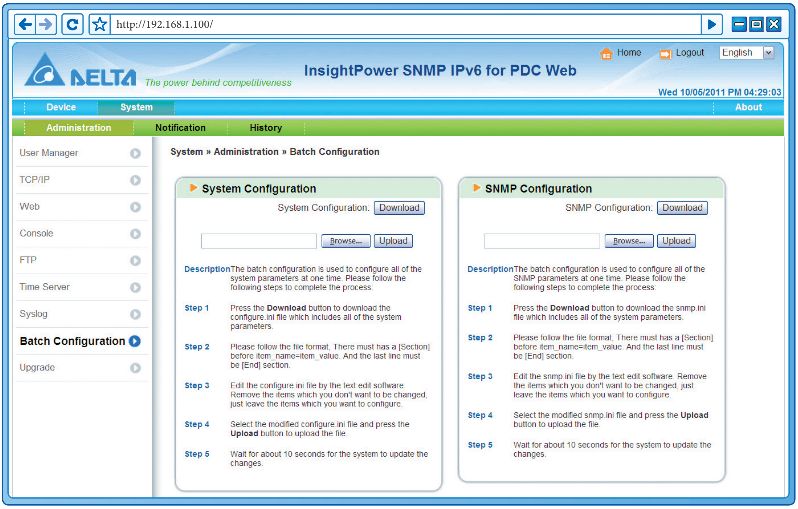
Syslog Server 2:

Syslog Server 3:

Syslog Server 4:

Submit

Batch Configuration



System » Administration » Batch Configuration

System Configuration

System Configuration: Download

Browse... Upload

Description The batch configuration is used to configure all of the system parameters at one time. Please follow the following steps to complete the process:

Step 1 Press the **Download** button to download the configure.ini file which includes all of the system parameters.

Step 2 Please follow the file format, There must has a [Section] before item_name=item_value. And the last line must be [End] section.

Step 3 Edit the configure.ini file by the text edit software. Remove the items which you don't want to be changed, just leave the items which you want to configure.

Step 4 Select the modified configure.ini file and press the **Upload** button to upload the file.

Step 5 Wait for about 10 seconds for the system to update the changes.

SNMP Configuration

SNMP Configuration: Download

Browse... Upload

Description The batch configuration is used to configure all of the SNMP parameters at one time. Please follow the following steps to complete the process:

Step 1 Press the **Download** button to download the snmp.ini file which includes all of the system parameters.

Step 2 Please follow the file format, There must has a [Section] before item_name=item_value. And the last line must be [End] section.

Step 3 Edit the snmp.ini file by the text edit software. Remove the items which you don't want to be changed, just leave the items which you want to configure.

Step 4 Select the modified snmp.ini file and press the **Upload** button to upload the file.

Step 5 Wait for about 10 seconds for the system to update the changes.

The batch configuration offers quick and effortless setup on multiple SNMP IPv6 units. After system configuration is completed, export configuration file and import on other units to duplicate settings and parameters.

- **System Configuration**

  This includes settings saved under the **System → administration** tab. To download a configuration file, simply click **Download** (configure.ini). To upload a configuration file, click **Browse**, select the configuration file you wish to upload, and click **Upload**.

NOTE

If you assign a static IP to your SNMP IPv6, open the configuration file with a text editor (such as Notepad or Word Pad), under the [System] section, remove the following line **IP=xxx.xxx.xxx.xxx**. To modify/ assign IP address for the SNMP IPv6, please see ***Chapter 4: System Configurations.***

- **SNMP Configuration**

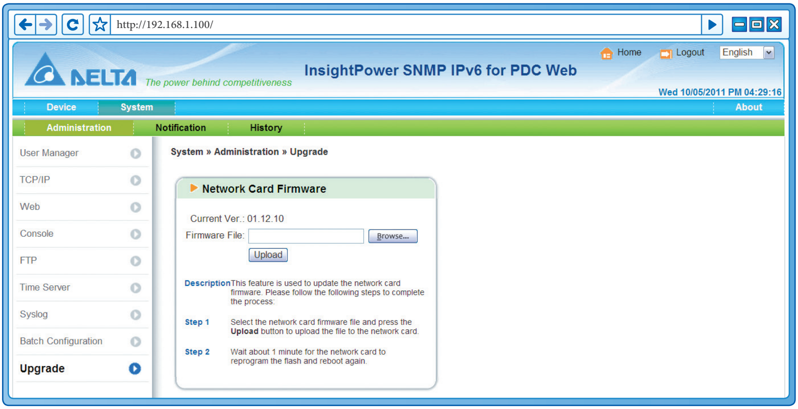
  This includes settings under the **System → Notification** tab. To download a configuration file, simply click **Download**. To upload a configuration file, click **Browse**, select the file you wish to upload, and click **Upload**.

NOTE

Follow the instructions shown on this page to modify the configuration files.

Upgrade

In this page, upgrade SNMP IPv6's firmware and check the current firmware version. Click **Browse,** choose the firmware patch file, and click **Upload**. The upgrade process should take about one minute to complete.



System » Administration » Upgrade

Network Card Firmware

Current Ver.: 01.12.10

Firmware File:

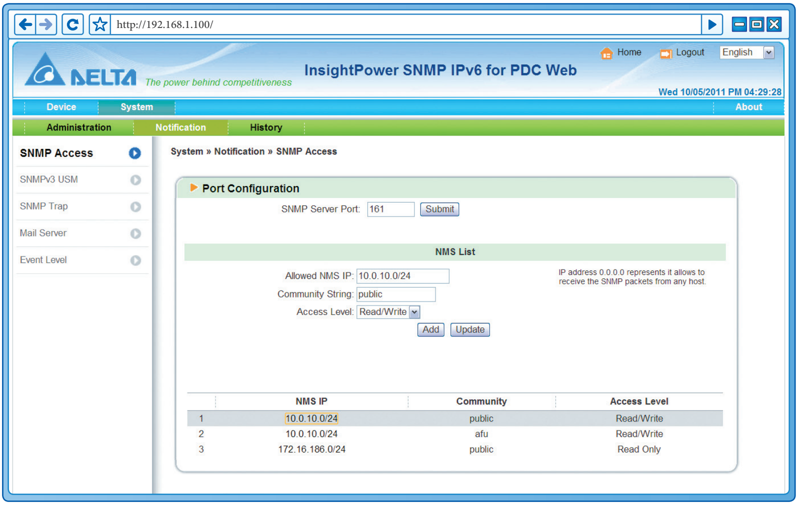
Description This feature is used to update the network card firmware. Please follow the following steps to complete the process:

Step 1 Select the network card firmware file and press the **Upload** button to upload the file to the network card.

Step 2 Wait about 1 minute for the network card to reprogram the flash and reboot again.

5-2-2 Notification

SNMP Access



System » Notification » SNMP Access

Port Configuration

SNMP Server Port: 161

NMS List

Allowed NMS IP: 10.0.10.0/24

Community String: public

Access Level: Read/Write

IP address 0.0.0.0 represents it allows to receive the SNMP packets from any host.

	NMS IP	Community	Access Level
1	10.0.10.0/24	public	Read/Write
2	10.0.10.0/24	afu	Read/Write
3	172.16.186.0/24	public	Read Only

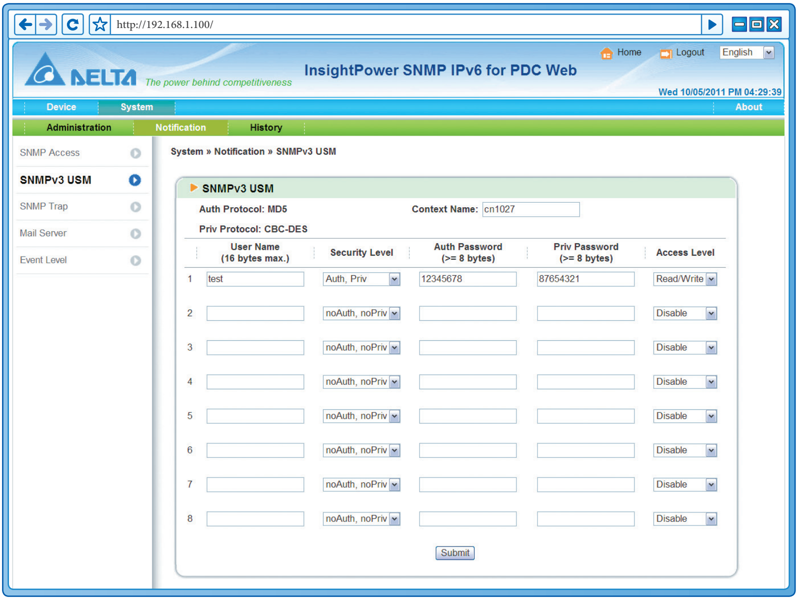
The SNMP IPv6 supports SNMP protocol and SNMP NMS (Network Management System), which are commonly used to monitor network devices for situations that call for administrative attention. To prevent unauthorized access, specify the allowed NMS IP addresses, their respective community strings and access levels. You can assign up to 256 IP addresses.

NOTE

If IP address 0.0.0.0 is added to the list, the NMS IP access restriction is ignored. SNMP IPv6 will check the community string to identify the access level and permission according to your settings.

SNMPv3 USM

The SNMPv3 protocol features packet encryption and user authentication to improve connection security. The SNMPv3 USM (User Session Management) allows you to assign eight user names whose access privileges are granted via the SNMPv3 protocol. Specify the user name, security level, auth/ priv passwords and access level for each account respectively.



System » Notification » SNMPv3 USM

SNMPv3 USM

Auth Protocol: MD5

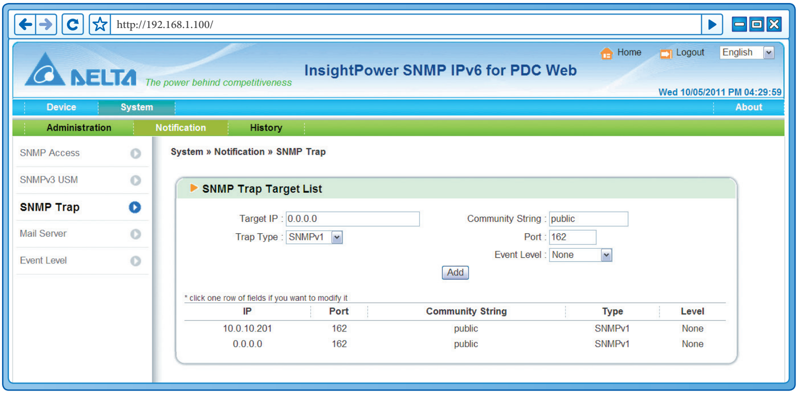
Context Name: cn1027

Priv Protocol: CBC-DES

	User Name (16 bytes max.)	Security Level	Auth Password (>= 8 bytes)	Priv Password (>= 8 bytes)	Access Level
1	test	Auth, Priv	12345678	87654321	Read/Write
2		noAuth, noPriv			Disable
3		noAuth, noPriv			Disable
4		noAuth, noPriv			Disable
5		noAuth, noPriv			Disable
6		noAuth, noPriv			Disable
7		noAuth, noPriv			Disable
8		noAuth, noPriv			Disable

SNMP Trap

SNMP Trap alerts users to event occurrences. To enable SNMP Trap, add Target IP addresses to the list. Specify the community string, port, trap type and event level, then click **Add**. Click on an entry to update settings or remove it from the list.



System » Notification » SNMP Trap

SNMP Trap Target List

Target IP : 0.0.0.0

Trap Type : SNMPv1

Community String : public

Port : 162

Event Level : None

Add

* click one row of fields if you want to modify it

IP	Port	Community String	Type	Level
10.0.10.201	162	public	SNMPv1	None
0.0.0.0	162	public	SNMPv1	None

NOTE

SNMPv1, SNMPv2c and SNMPv3 Traps are supported. If the SNMPv3 Trap is enabled, the user names must be specified in SNMPv3 USM.

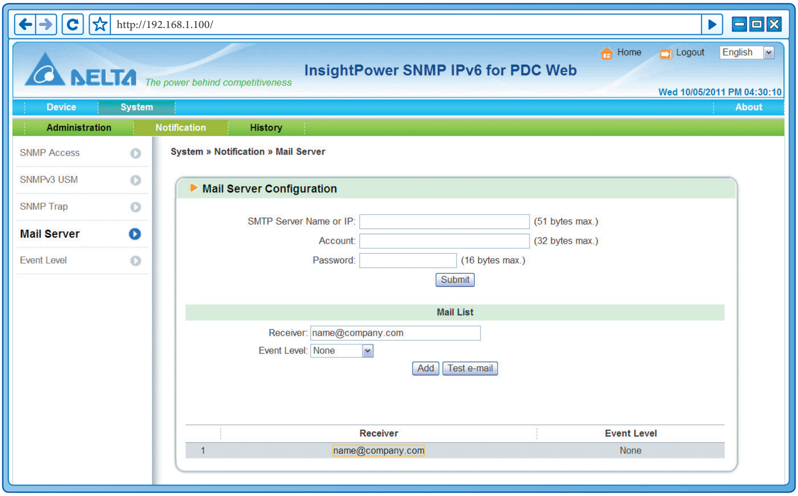
The target IP addresses receive event notifications based on the event levels you specified. Three event levels are shown as follows:

- **Information :** All event notifications are sent to the target address.
- **Warning :** Warning and alarm event notifications are sent to the target address.
- **Alarm :** Only alarm event notifications are sent to the target address.

Click **Event Level** on the left panel to change event levels for individual events.

Mail Server

Configure an SMTP server to send event notifications to recipients specified on the mail list. Up to 256 recipients can be added.



SMTP Server Name or IP: (51 bytes max.)

Account: (32 bytes max.)

Password: (16 bytes max.)

Receiver: name@company.com

Event Level: None

	Receiver	Event Level
1	name@company.com	None

NOTE

If a DNS server is not available in the network, you need to manually assign an SMTP server address to enable the E-mail notification system.

- If a Host Name is entered in **SMTP Server Name or IP**, a DNS IP address should be added in the TCP/ IP page.

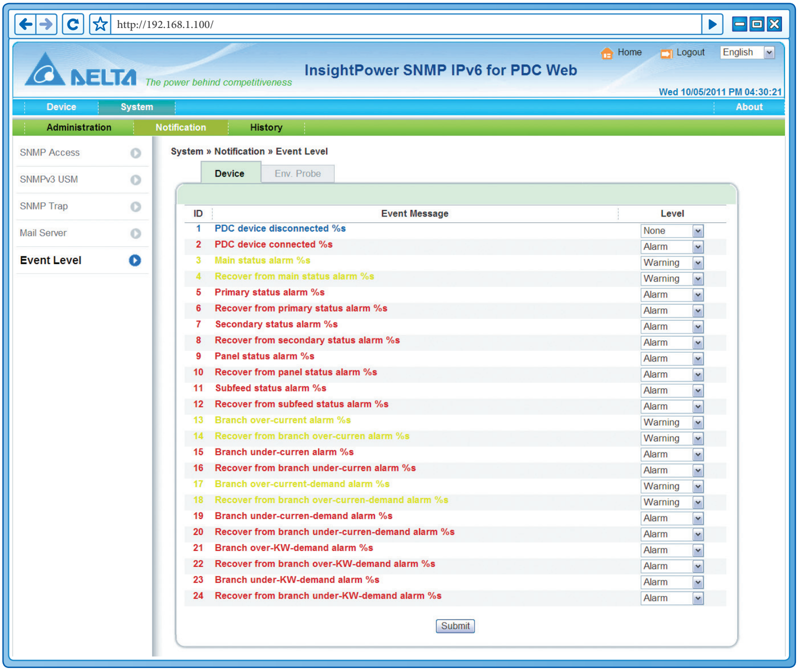
  Specify the e-mail address and event level. When an event occurs, a notification will be sent to the target address. Refer to the following:

  1) **Information :** All event notifications are sent to the target address.

  2) **Warning :** Warning and Alarm event notifications are sent to the target address.

  3) **Alarm :** Only alarm event notifications are sent to the target address.

Event Level



System » Notification » Event Level

ID	Event Message	Level
1	PDC device disconnected %s	None
2	PDC device connected %s	Alarm
3	Main status alarm %s	Warning
4	Recover from main status alarm %s	Warning
5	Primary status alarm %s	Alarm
6	Recover from primary status alarm %s	Alarm
7	Secondary status alarm %s	Alarm
8	Recover from secondary status alarm %s	Alarm
9	Panel status alarm %s	Alarm
10	Recover from panel status alarm %s	Alarm
11	Subfeed status alarm %s	Alarm
12	Recover from subfeed status alarm %s	Alarm
13	Branch over-current alarm %s	Warning
14	Recover from branch over-curren alarm %s	Warning
15	Branch under-curren alarm %s	Alarm
16	Recover from branch under-curren alarm %s	Alarm
17	Branch over-current-demand alarm %s	Warning
18	Recover from branch over-curren-demand alarm %s	Warning
19	Branch under-curren-demand alarm %s	Alarm
20	Recover from branch under-curren-demand alarm %s	Alarm
21	Branch over-KW-demand alarm %s	Alarm
22	Recover from branch over-KW-demand alarm %s	Alarm
23	Branch under-KW-demand alarm %s	Alarm
24	Recover from branch under-KW-demand alarm %s	Alarm

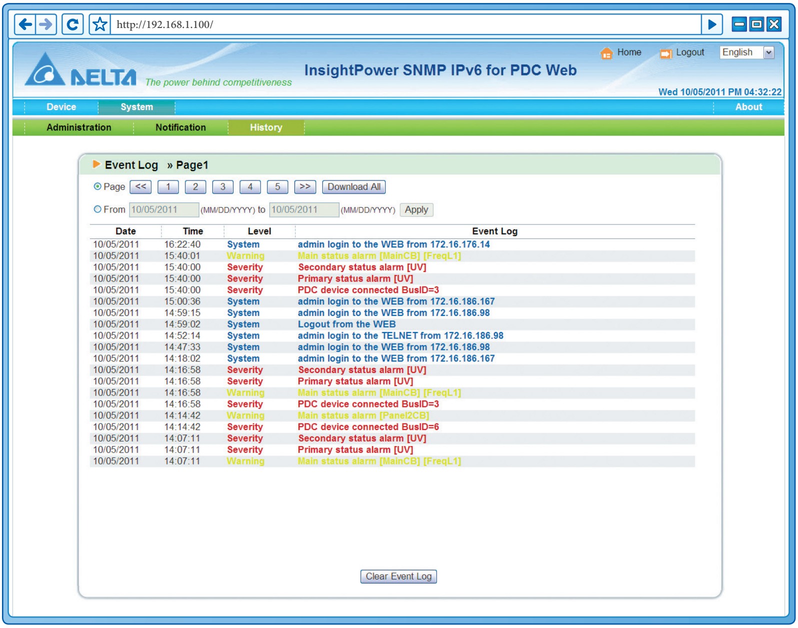
- **Device :** Three event levels, including information (blue), warning (yellow) and alarm (red) can be assigned to PDC's events. Click **Submit** to take effect.
- **Env.Probe :** Assign event levels to EnviroProbe's events. Click **Submit** to take effect.

5-2-3 History

In this page, check event entries. Click << and >> to turn pages. Click on a page number to jump to that page.

To check event entries recorded during a time period, select the dates and click **Apply**. To download the entire event log, click **Download All** and a pop-up window prompts you to save the file (.csv). You can open or edit the file in Microsoft Excel.

Click **Clear Event Log** to erase all event entries. It is recommended to download and back up your event log first.



Event Log » Page1

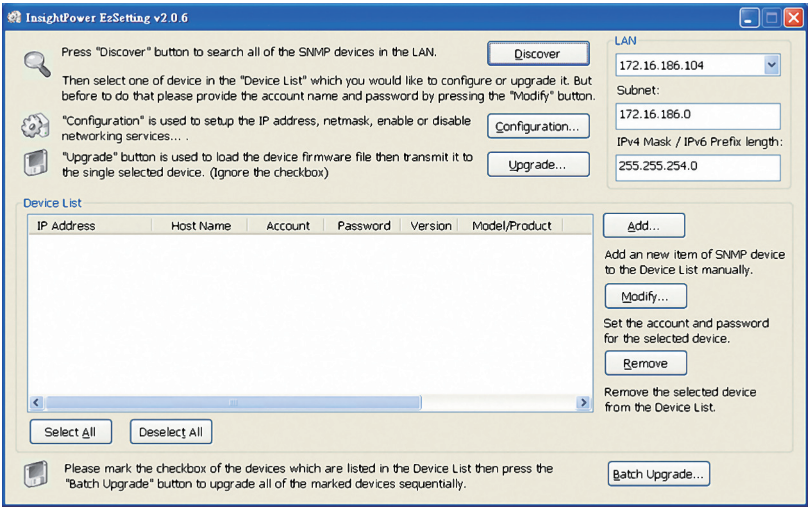
● Page << 1 2 3 4 5 >> Download All

○ From 10/05/2011 (MM/DD/YYYY) to 10/05/2011 (MM/DD/YYYY) Apply

Date	Time	Level	Event Log
10/05/2011	16:22:40	System	admin login to the WEB from 172.16.176.14
10/05/2011	15:40:01	Warning	Main status alarm [MainCB] [FreqL1]
10/05/2011	15:40:00	Severity	Secondary status alarm [UV]
10/05/2011	15:40:00	Severity	Primary status alarm [UV]
10/05/2011	15:40:00	Severity	PDC device connected BusID=3
10/05/2011	15:00:36	System	admin login to the WEB from 172.16.186.167
10/05/2011	14:59:15	System	admin login to the WEB from 172.16.186.98
10/05/2011	14:59:02	System	Logout from the WEB
10/05/2011	14:52:14	System	admin login to the TELNET from 172.16.186.98
10/05/2011	14:47:33	System	admin login to the WEB from 172.16.186.98
10/05/2011	14:18:02	System	admin login to the WEB from 172.16.186.167
10/05/2011	14:16:58	Severity	Secondary status alarm [UV]
10/05/2011	14:16:58	Severity	Primary status alarm [UV]
10/05/2011	14:16:58	Warning	Main status alarm [MainCB] [FreqL1]
10/05/2011	14:16:58	Severity	PDC device connected BusID=3
10/05/2011	14:14:42	Warning	Main status alarm [Panel2CB]
10/05/2011	14:14:42	Severity	PDC device connected BusID=6
10/05/2011	14:07:11	Severity	Secondary status alarm [UV]
10/05/2011	14:07:11	Severity	Primary status alarm [UV]
10/05/2011	14:07:11	Warning	Main status alarm [MainCB] [FreqL1]

Chapter 6 : SNMP Device Firmware Upgrade

With the provided program EzSetting, you can effortlessly perform a firmware upgrade on your SNMP devices via LAN. Please refer to the following instructions.



Press "Discover" button to search all of the SNMP devices in the LAN.

Then select one of device in the "Device List" which you would like to configure or upgrade it. But before to do that please provide the account name and password by pressing the "Modify" button.

"Configuration" is used to setup the IP address, netmask, enable or disable networking services... .

"Upgrade" button is used to load the device firmware file then transmit it to the single selected device. (Ignore the checkbox)

LAN: 172.16.186.104

Subnet: 172.16.186.0

IPv4 Mask / IPv6 Prefix length: 255.255.254.0

Device List

IP Address	Host Name	Account	Password	Version	Model/Product

Add an new item of SNMP device to the Device List manually.

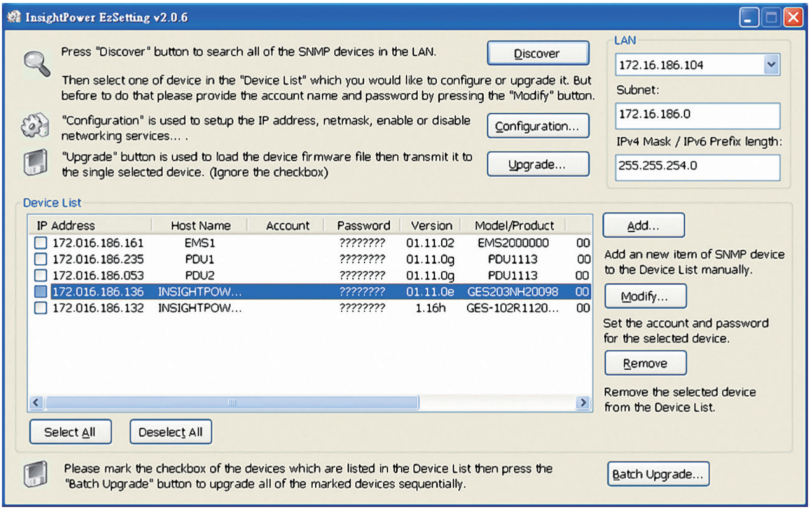
Set the account and password for the selected device.

Remove the selected device from the Device List.

Please mark the checkbox of the devices which are listed in the Device List then press the "Batch Upgrade" button to upgrade all of the marked devices sequentially.

Step 1 The subnet mask allows you to define the device discovery range in the specified subnets. Make sure the SNMP device you wish to upgrade is in the subnet that is specified. If it is not, please modify the subnet and subnet mask.

Step 2 Click **Discover**. A list of SNMP devices is shown.



InsightPower EzSetting v2.0.6

Press "Discover" button to search all of the SNMP devices in the LAN.

Then select one of device in the "Device List" which you would like to configure or upgrade it. But before to do that please provide the account name and password by pressing the "Modify" button.

"Configuration" is used to setup the IP address, netmask, enable or disable networking services... .

"Upgrade" button is used to load the device firmware file then transmit it to the single selected device. (Ignore the checkbox)

LAN

172.16.186.104

Subnet:

172.16.186.0

IPv4 Mask / IPv6 Prefix length:

255.255.254.0

Device List

IP Address	Host Name	Account	Password	Version	Model/Product	
□ 172.016.186.161	EMS1		????????	01.11.02	EMS2000000	00
□ 172.016.186.235	PDU1		????????	01.11.0g	PDU1113	00
□ 172.016.186.053	PDU2		????????	01.11.0g	PDU1113	00
□ 172.016.186.136	INSIGHTPOW...		????????	01.11.0e	GES203NH20098	00
□ 172.016.186.132	INSIGHTPOW...		????????	1.16h	GES-102R1120...	00

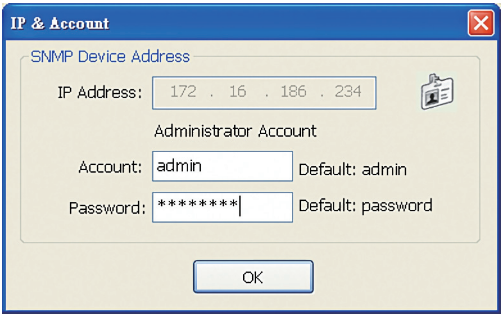
Add an new item of SNMP device to the Device List manually.

Set the account and password for the selected device.

Remove the selected device from the Device List.

Please mark the checkbox of the devices which are listed in the Device List then press the "Batch Upgrade" button to upgrade all of the marked devices sequentially.

Step 3 Select a device from the Device List, click **Modify**, and key in Administrator account and password.



IP & Account

SNMP Device Address

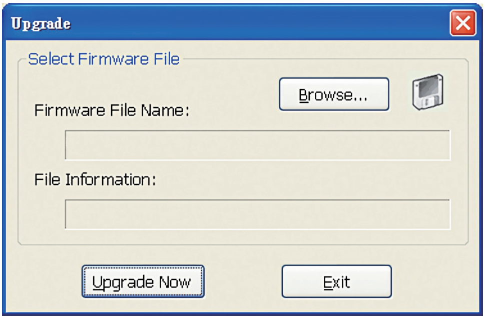
IP Address: 172 . 16 . 186 . 234

Administrator Account

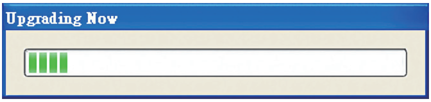
Account: admin Default: admin

Password: ******** Default: password

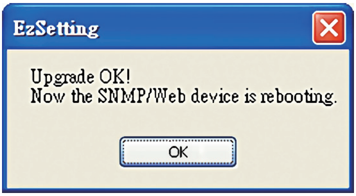
Step 4 Click **Upgrade**. The upgrade dialog box pops up. Click **Browse** to select a valid firmware binary file. Verify the firmware version shown under File Information, and then click **Upgrade Now** to continue.



Step 5 The upgrade process should take about 20 seconds.



Step 6 When the upgrade is completed, the following dialog box appears. It takes about 1 minute for the device to reboot.



EzSetting

Upgrade OK!
Now the SNMP/Web device is rebooting.

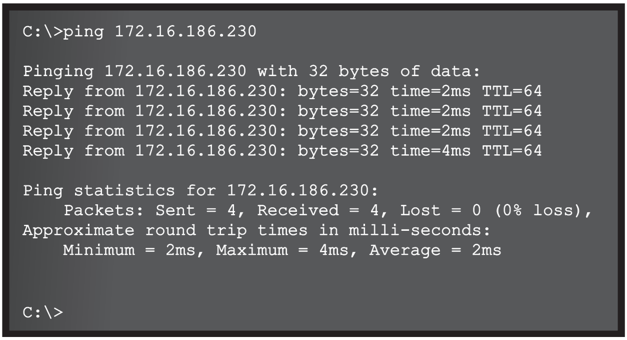
Chapter 7 : Troubleshooting

Q1. How to set up an SNTP server on my workstation for the SNMP IPv6 to synchronize?

To enable SNTP services in Windows XP, go to **Start** → **Control Panel** → **Add/ Remove Programs** → **Add/ Remove Windows Components** → **Networking Services** → check **Simple TCP/ IP Services** → **OK**. To enable time synchronization, you need to set SNTP time server addresses in **Time Server**. Please refer to ***Chapter 4: System Configurations***.

Q2. How to make sure the linking between the SNMP IPv6's and the PDC is established?

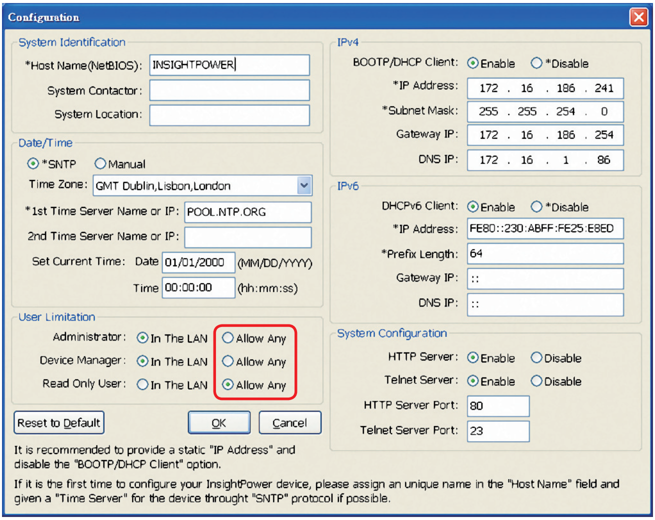
If the linking between the SNMP IPv6 and the PDC is correctly established, the yellow LED indicator should flash rapidly. If not, confirm that the device ID setting on the SNMP IPv6 and the PDC is consistent.



```
C:\>ping 172.16.186.230

Pinging 172.16.186.230 with 32 bytes of data:
Reply from 172.16.186.230: bytes=32 time=2ms TTL=64
Reply from 172.16.186.230: bytes=32 time=2ms TTL=64
Reply from 172.16.186.230: bytes=32 time=2ms TTL=64
Reply from 172.16.186.230: bytes=32 time=4ms TTL=64

Ping statistics for 172.16.186.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms


C:\>
```

Q3. I can access the InsightPower SNMP IPv6 for PDC Web, but I cannot login in.

Please check the IP addresses of the SNMP IPv6 and the workstation on which you are trying to log in. By default, they must be within the same LAN so you can connect via the web interface. You can enable external connections to solve this issue. To do this, launch EzSetting and change User Limitation to Allow Any, as shown below.



System Identification

*Host Name(NetBIOS): INSIGHTPOWER

System Contactor:

System Location:

Date/Time

● *SNTP ○ Manual

Time Zone: GMT Dublin,Lisbon,London

*1st Time Server Name or IP: POOL.NTP.ORG

2nd Time Server Name or IP:

Set Current Time: Date 01/01/2000 (MM/DD/YYYY)

Time 00:00:00 (hh:mm:ss)

User Limitation

Administrator: ● In The LAN ○ Allow Any

Device Manager: ● In The LAN ○ Allow Any

Read Only User: ○ In The LAN ● Allow Any

It is recommended to provide a static "IP Address" and disable the "BOOTP/DHCP Client" option.

IPv4

BOOTP/DHCP Client: ● Enable ○ *Disable

*IP Address: 172 . 16 . 186 . 241

*Subnet Mask: 255 . 255 . 254 . 0

Gateway IP: 172 . 16 . 186 . 254

DNS IP: 172 . 16 . 1 . 86

IPv6

DHCPv6 Client: ● Enable ○ *Disable

*IP Address: FE80::230:ABFF:FE25:E8ED

*Prefix Length: 64

Gateway IP: ::

DNS IP: ::

System Configuration

HTTP Server: ● Enable ○ Disable

Telnet Server: ● Enable ○ Disable

HTTP Server Port: 80

Telnet Server Port: 23

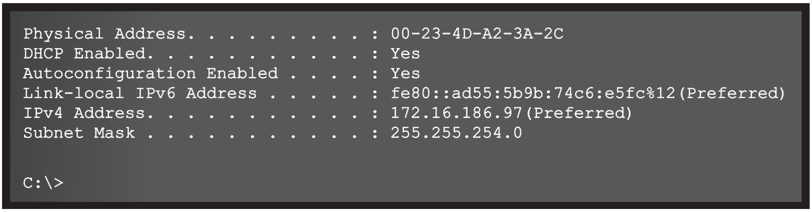
If it is the first time to configure your InsightPower device, please assign an unique name in the "Host Name" field and given a "Time Server" for the device throught "SNTP" protocol if possible.

Q4. Unable to connect to the SNMP IPv6 via its Host Name?

If you just assign a new static IP address to the SNMP IPv6, you may need to refresh the NetBIOS table so that it corresponds with the new setting. Although Windows updates its NetBIOS table periodically, you can still manually force it to refresh by entering the following command **nbtstat –R** in DOS prompt mode. After that, you can now connect to the SNMP IPv6 by its Host Name. Please also ensure that the Host Name assigned to the SNMP IPv6 does not exceed 16 bytes.

Q5. How to check my workstation's IP address?

For Windows, please enter **ipconfig /all** in DOS prompt mode. For UNIX, please enter **ifconfig** in shell. You should be able to check your IP and MAC (Physical Address) now.



```
Physical Address. . . . . . . . . : 00-23-4D-A2-3A-2C
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::ad55:5b9b:74c6:e5fc%12(Preferred)
IPv4 Address. . . . . . . . . . . : 172.16.186.97(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.254.0

C:\>
```

Q6. Unable to ping the SNMP IPv6 from my workstation?

If the SNMP IPv6 is non-responsive, check the following:

1) If the green LED indicator on the SNMP IPv6 is OFF, check if the network cable is correctly connected from the SNMP IPv6 to the router or hub.

2) If the green LED indicator is ON, the current IP address could be unreachable. Manually assign a valid IP address to the SNMP IPv6.

3) If the green LED indicator flashes and (1) your network configuration includes a DHCP server, make sure the DHCP service is working properly; (2) Otherwise, make sure the assigned IP is not already taken on the network. Please note that if the current configuration is not useable, the SNMP IPv6 will reset to default IP settings (IPv4 address: 192.168.1.100/ net mask: 255.255.255.0/ gateway: 192.168.1.254).

4) If the problem persists, use a network cable to cross link your SNMP IPv6 and the workstation. Ping the SNMP IPv6's default or static IP address, according to your configurations. If a ping response is successfully received, indicating that the SNMP IPv6 is working properly, check your network equipment. If not, contact your local dealer or service personnel for assistance.

Q7. Unable to perform an SNMP Get command?

Refer to ***5-2-2 Notification*** to check SNMP settings. Make sure that the workstation's IP address is added to the NMS IP list with Read or Read/ Write access. The community string on the workstation and the SNMP IPv6 must match.

Q8. Unable to perform an SNMP Set command?

Refer to ***5-2-2 Notification*** to check SNMP settings. Make sure that the workstation's IP address is added to the NMS IP list, with Read/ Write permission. The community string on the PC and the SNMP IPv6 must match.

Q9. Unable to receive SNMP trap?

Refer to ***5-2-2 Notification*** to check SNMP Trap settings. Make sure that the workstation's IP address is added to the Target IP list.

Q10. Forgot Administrator's account and password?

You can reset Administrator's account and password via text mode. Refer to ***4-4 Configuring via COM*** Port to establish a COM port connection with the SNMP IPv6. When the login information is prompted, key in **rstadmin** within 30 seconds and press **enter**. The Administrator account and password are now reset to default (admin/ password).

Q11. How to enable IPv6 in Windows XP?

If you are running Windows XP, please enable IPv6 first (click **START → RUN**, and enter **ipv6 install**). The SNMP IPv6 supports IPv6 with no additional configurations required. However, please note that IPv6 is automatically disabled if an identical LLA (Local-link Address) already exists on the LAN. If the SNMP IPv6 obtains both IPv4 and IPv6 records from DNS resolution, the IPv4 is used as the primary IP address for the given Host Name.

To learn more information regarding IPv6 compatibility, please visit IETF (http://tools.ietf.org/html), or IPv6 Ready Logo Program (http://www.ipv6ready.org).

Q12. How to generate a private SSL certificate file (in PEM format) for HTTPs connection?

To ensure connection security between the SNMP IPv6 and your workstation, you can create your own SSL certificate file. Please download and install OpenSSL Toolkit from http://www.openssl.org. Launch Shell or DOS prompt mode and enter the following command to create your own certificate file:

```
openssl req -x509 -nodes -days 3650 -newkey
rsa:1024 -keyout cert.pem -out cert.pem
```

1) Answer the prompted questions. Proceed with the given directions. Once it is completed, a file named cert.pem is created in the current working directory.

2) Upload cert.pem to the InsightPower SNMP IPv6 for PDC Web. Please refer to ***5-2-1 Administration – Web***.

Q13. How to generate DSA, RSA and Public keys for SSH?

For Linux:

1) Please download and install OpenSSH from http://www.openssh.org.

2) Launch Shell and enter the following commands to create your own keys (please ignore it when prompted to provide passphrase):

```
DSA Key:ssh-keygen -t dsa
RSA Key:ssh-keygen -t rsa
```

3) Upload DSA and RSA keys to the InsightPower SNMP IPv6 for PDC Web. Please refer to ***5-2-1 Administration – Console*** for more information.

For Windows:

1) Please download and install PuTTY from http://www.putty.org.

2) Run puttygen.exe from the installed directory.

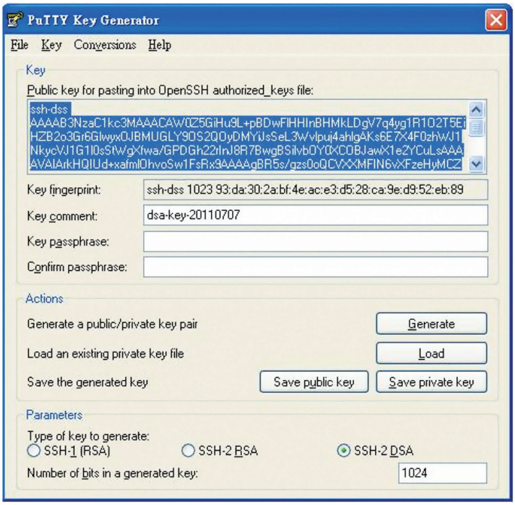
3) Select **SSH-2 RSA** from the Parameters area and click **Key** → **Generate key pair** to generate a RSA key.

4) Click **Conversions** → **Export OpenSSH Key** and assign a filename to the RSA key. Please ignore it when prompted to provide key passphrase.

5) Select **SSH-2 DSA** from the Parameters, clickt **Key** → **Generate key pair** to generate a DSA key.

6) Click **Conversions** → **Export OpenSSH Key** and assign a filename to the DSA key. Please ignore it when prompted to provide key passphrase.

7) Copy the generated key from the text box, paste in a text editor and save as a text file.



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-dss
AAAAB3NzaC1kc3MAAACAW0Z5GiHu9L+pBDwFlHHInBHMkLDgV7q4yg1R102T5Ei
HZB2o3Gr6GlwyxOJBMUGLY90S2QOyDMYiJsSeL3Wvlpuj4ahlgAKs6E7X4F0zhWJ1
NkycVJ1G1l0sStWgXfwa/GPDGh22rlnJ8R7BwgBSilvbOY0XC0BJawX1e2YCuLsAAA
AVAIArkHQIUd+xafml0hvoSw1FsRx9AAAAgBR5s/gzs0oQCVXXMFIN6vXFzeHyMCZ
```

Key fingerprint: ssh-dss 1023 93:da:30:2a:bf:4e:ac:e3:d5:28:ca:9e:d9:52:eb:89

Key comment: dsa-key-20110707

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ○ SSH-2 RSA ● SSH-2 DSA

Number of bits in a generated key: 1024

8) Upload the DSA/ RSA/ Public keys files to the InsightPower SNMP IPv6 for PDC Web. Refer to ***5-2-1 Administrator – Console*** for more information.

Q14. How to upload configuration / firmware / key files via SSH/ SFTP?

To quickly configure your SNMP IPv6, you can upload the files via SSH/ SFTP. The SNMP IPv6 automatically imports your settings after the files are uploaded to the designated directories. Refer to the following table:

Directory	Files
\config_snmp	snmp.ini
\config_system	configure.ini
\ssh_dsa	DSA key
\ssh_rsa	RSA key
\ssh_pubkey	Public key
\upgrade_snmp	SNMP IPv6's firmware upgrade package (binary)
\upgrade_device*	Device's firmware upgrade package (binary)

*Appears on specific devices only.

Upload files to their respective directories. Make sure the filenames do not contain non-English characters to avoid read error. Overwrite existing files if prompted by your SFTP client.

Q15. How to test SNMPv3 in Linux?

Before you can access the SNMP OID (Object Identifier) via SNMPv3 protocol, the SNMPv3 USM table must be organized. Please refer to ***5-2-2 Notification – SNMPv3 USM*** for more information.

To test SNMPv3 in Linux, launch shell and key in the following command:

```
snmpwalk -v 3 -u <user> -l authPriv -A <pass-
word> -X <password> -n <context name> -t 3 <ip>
1.3.6.1.2.1.1.1.0
```

-v: 1 for SNMPv1, 3 for SNMPv3.

-l: Follow the security levels. They are: noAuthNoPriv, authNoPriv and authPriv.

-u: The user name which is assigned from SNMPv3 USM table.

-A: The Auth Password which is assigned from SNMPv3 USM table.

-X: The Priv Password which is assigned from SNMPv3 USM table.

-n: The Context Name which is assigned from SNMPv3 USM table.

-t: Timeout in seconds.

<ip>: The IP address of the SNMP IPv6.

<oid>: The next available SNMP OID (for example: 1.3.6.1.2.1.1.1.0). Please refer to the RFC1213 MIB.

Appendix A : Specifications

Model Name	InsightPower SNMP IPv6 for PDC
Power Input	12 Vdc
Power Consumption	2 Watt (Max.)
Network Connection	RJ-45 jack connector (10/ 100M)
Physical	
Size (W x D)	130 mm x 60 mm
Weight	75 g
Environmental	
Operating Temperature	0 ~ 60℃
Storage Temperature	-40 ~ 125℃
Operating Humidity	0 ~ 90 % (Non-condensing)

NOTE

＊ Refer to the rating label for the safety rating.
＊ All specifications are subject to change without prior notice.

Appendix B : Warranty

Seller warrants this product, if used in accordance with all applicable instructions, to be free from original defects in material and workmanship within the warranty period. If the product has any failure problem within the warranty period, Seller will repair or replace the product at its sole discretion according to the failure situation.

This warranty does not apply to normal wear or to damage resulting from improper installation, operation, usage, maintenance or irresistible force (i.e. war, fire, natural disaster, etc.), and this warranty also expressly excludes all incidental and consequential damages.

Maintenance service for a fee is provided for any damage out of the warranty period. If any maintenance is required, please directly contact the supplier or Seller.

WARNING : The individual user should take care to determine prior to use whether the environment and the load characteristic are suitable, adequate or safe for the installation and the usage of this product. The User Manual must be carefully followed. Seller makes no representation or warranty as to the suitability or fitness of this product for any specific application.